



60386

D 001441

TANICZNA

codificare
decodificare

13 VOLUME

Pentru uz intern

CODIFICARE, DECODIFICARE

Seria 1020

1970

DIN PARTEA REDACȚIEI

Lucrarea „Codificare, decodificare” are menirea de a prezenta cititorilor unele aspecte din evoluția, de-a lungul veacurilor, a unei științe cu tente de mister, ce a fascinat și a atras imaginația celor mai diverse minți, născute în civilizațiile care au stăruit pe meridianele globului.

Apărută pe malurile Nilului, criptologia avea să răspundă nevoii de a apăra și de a afla secrete ce constituiau interese vitale ale unor țări, popoare, grupări sociale, politice, religioase etc. Astfel, încă de la început, s-au conturat cele două componente de bază ale noii științe și anume: criptografia și criptanaliza. Scopul criptografiei este ca, prin transformarea deliberată a scrisului, să se ascundă înțelesul unor mesaje față de cei ce nu trebuie să-l cunoască, iar criptanaliza urmărește să descopere această transformare. Rezultă, deci, interdependența dintre aceste două ramuri ale criptologiei, fiind foarte ușor de înțeles că orice schimbare, în sens progresiv, în una dintre ele atrage după sine schimbări evolutive și în cealaltă. O astfel de axiomă este ilustrată de istoria criptologiei, căci, de la elementele primare, cuprinse în culturile antice, până la mașinile electronice din zilele noastre, a fost parcurs un drum în general ascendent, presărat, însă, cu multe suișuri și coborișuri abrupte.

În această lucrare sint prezentate numai momentele de ascensiune ale criptologiei. S-a procedat în acest mod, pe de o parte, pentru a prezenta sistematic și logic dezvoltarea, de-a

lungul timpului, a celor două ramuri ale criptologiei, iar pe de altă parte, pentru a ajuta la o mai bună înțelegere a sistemelor, procedeeelor și metodelor de criptare și decriptare moderne, respectându-se principiul didactic, conform căruia, în însușirea unor cunoștințe, trebuie să se pornească de la simplu pentru a se ajunge la complex.

Scopul lucrării este, deci, să-l înarmeze pe cititor cu o serie de cunoștințe din domeniul cifrurilor, codurilor și al altor procedee folosite în scrierile ascunse.

Ea are menirea să stimuleze interesul față de acest domeniu de activitate și să atragă atenția asupra pericolului ce rezidă în tratarea cu superficialitate a măsurilor de apărare a secretelor de partid, de stat și militare, indicând armele care stau la dispoziția oricui este interesat să apere sau să intre în posesia acestor secrete.

Din lucrare emană, de asemenea, caracterul evolutiv al criptologiei, fapt care îndeamnă pe fiecare să încerce să-și aducă contribuția activă la dezvoltarea acestei științe, atât prin elaborarea unor noi sisteme de criptare, cât și prin găsirea unor metode ingenioase de soluționare a criptogramelor și scrierilor ascunse, folosite în mod curent în activitatea subversivă.

NAȘTEREA CRIPTOLOGIEI

PRIMI 3 000 DE ANI

Cu aproape 4 000 de ani în urmă, într-un oraș numit Menet Khufu, de pe malul Nilului, un scrib, desenând hieroglife, povestea viața stăpinului său și — făcând acest lucru — scria primele rînduri din istoria criptologiei.

Nu era vorba de un sistem de scriere secretă de tipul celui cunoscut de lumea modernă, ci de folosirea unor hieroglife mai deosebite pentru a proslăvi faptele stăpinului. De asemenea, intenția lui nu era să facă textul de neînțeles, ci să-i acorde grandoare, demnitate și autoritate. Deci, nu se poate spune că acest text constituia o scriere secretă, dar el încorporează unul din elementele esențiale ale criptografiei: transformarea deliberată a scrisului.

Cu timpul, textele de acest gen s-au înmulțit, transformările s-au complicat și n-a trecut mult pînă cînd a apărut și cel de-al doilea element esențial al criptologiei: secretul.

Transformarea scrierii și secretul au dus la criptografie, deși la început aceasta se asemăna mai mult cu un joc prin care se urmărea să se întîrzie înțelegerea textului, iar criptanaliza nu era altceva decît rezolvarea unui rebus.

Așa a apărut criptologia, care, timp de 3 000 de ani, s-a dezvoltat, mai mult independent, în diferite părți ale lumii și multe realizări din acest domeniu au dispărut o dată cu apusul

lungul timpului, a celor două ramuri ale criptologiei, iar pe de altă parte, pentru a ajuta la o mai bună înțelegere a sistemelor, procedeeelor și metodelor de criptare și decriptare moderne, respectându-se principiul didactic, conform căruia, în însușirea unor cunoștințe, trebuie să se pornească de la simplu pentru a se ajunge la complex.

Scopul lucrării este, deci, să-l înarmeze pe cititor cu o serie de cunoștințe din domeniul cifrurilor, codurilor și al altor procedee folosite în scrierile ascunse.

Ea are menirea să stimuleze interesul față de acest domeniu de activitate și să atragă atenția asupra pericolului ce rezidă în tratarea cu superficialitate a măsurilor de apărare a secretelor de partid, de stat și militare, indicând armele care stau la dispoziția oricui este interesat să apere sau să intre în posesia acestor secrete.

Din lucrare emană, de asemenea, caracterul evolutiv al criptologiei, fapt care îndeamnă pe fiecare să încerce să-și aducă contribuția activă la dezvoltarea acestei științe, atât prin elaborarea unor noi sisteme de criptare, cât și prin găsirea unor metode ingenioase de soluționare a criptogramelor și scrierilor ascunse, folosite în mod curent în activitatea subversivă.

NAȘTEREA CRIPTOLOGIEI

PRIMI 3 000 DE ANI

Cu aproape 4 000 de ani în urmă, într-un oraș numit Menet Khufu, de pe malul Nilului, un scrib, desenând hieroglife, povestea viața stăpinului său și — făcând acest lucru — scria primele rinduri din istoria criptologiei.

Nu era vorba de un sistem de scriere secretă de tipul celui cunoscut de lumea modernă, ci de folosirea unor hieroglife mai deosebite pentru a proslăvi faptele stăpinului. De asemenea, intenția lui nu era să facă textul de neînțeles, ci să-i acorde grandoare, demnitate și autoritate. Deci, nu se poate spune că acest text constituia o scriere secretă, dar el încorporează unul din elementele esențiale ale criptografiei: transformarea deliberată a scrisului.

Cu timpul, textele de acest gen s-au înmulțit, transformările s-au complicat și n-a trecut mult până când a apărut și cel de-al doilea element esențial al criptologiei: secretul.

Transformarea scrierii și secretul au dus la criptografie, deși la început aceasta se asemăna mai mult cu un joc prin care se urmărea să se întârzie înțelegerea textului, iar criptanaliza nu era altceva decât rezolvarea unui rebus.

Așa a apărut criptologia, care, timp de 3 000 de ani, s-a dezvoltat, mai mult independent, în diferite părți ale lumii și multe realizări din acest domeniu au dispărut o dată cu apusul

unor civilizații. În alte părți, criptologia a supraviețuit, a intrat în cultura poporului respectiv și a continuat să progreseze. Dar progresul a fost anevoios și în salturi. Mai mult s-a pierdut decât s-a reținut. Abia în perioada Renașterii europene a început să se înalțe monumentul criptografic.

China, țara cu o cultură antică destul de dezvoltată, nu a acordat prea mare atenție criptografiei. Diplomații și autoritățile militare chineze se foloseau de curieri care memorau mesajele ce le aveau de transmis, iar pentru mesajele scrise foloseau mătase și hirtie foarte subțire, care erau făcute cocoloș și învelite cu ceară. Curierul ascundea cocoloșul de ceară (de multe ori în rectum) sau îl înghițea, ducându-l astfel la destinatar.

Criptografia implica de cele mai multe ori folosirea unor coduri simple. De exemplu, dacă în numele unei persoane era inclusă ideograma „crizantemă”, acesteia i se spunea codificat „floarea galbenă”.

Pentru scopuri militare, în secolul al XI-lea, într-o compilație denumită „Problemele esențiale ale scrierilor clasice militare” se recomanda un cod, în accepțiunea modernă a cuvintului. Astfel, pentru o listă de 40 de noțiuni în text clar: ocereri de săgeți și arcuri, raportarea despre obținerea unei victorii etc. se foloseau primele 40 de ideograme ale unui poem. În cazul în care un comandant avea nevoie de săgeți, scria ideograma din poem corespunzătoare acestei noțiuni într-un anumit loc dintr-un mesaj obișnuit, îl sigila și-l trimitea celor în drept să-l primească. Răspunsul era dat sub aceeași formă. Dacă se întâmpla să cadă în mîna inamicului, mesajul respectiv nu putea fi descifrat decât dacă i se cunoștea codul. Cu toate acestea, în ciuda înaltei sale civilizații, China n-a strălucit prin realizări în domeniul criptologiei. Explicația constă și în aceea că scrierea chinezească, deși foarte veche, era foarte grea și cei care știau să o citească erau foarte puțini.

În India, de asemenea, se cunoșteau și, se pare, se practicau mai multe forme de comunicări secrete. Kautilya, presupusul autor al lucrării Artha-sastra, descriind serviciul de informații

al Indiei, recomanda ofițerilor de spionaj să folosească scrierea secretă cînd dădeau misiuni agenților și spionilor. Pe de altă parte, recomanda ambasadurilor să folosească criptanaliza pentru a obține informații „decriptînd desenele și scrierile secrete”.

Deși nu dă nici o metodă prin care puteau fi decriptate desenele și scrierile ascunse, faptul că vorbește despre soluțiile posibile ale acestora înseamnă că criptanaliza atinsese un stadiu destul de avansat. Oricum, este prima referire din istorie la criptanaliză folosită în scopuri politice.

Dar poate cea mai interesantă lucrare pentru criptologie este Kama-sutra, un manual de erotică, în care scrierea secretă este trecută ca una din cele 64 de arte pe care trebuie să le cunoască și să le practice femeile.

Se descriu două feluri de scriere secretă și anume: unul numit „Kautilyam”, în care substituția literelor este bazată pe relații fonetice (vocalele devin consoane și invers), iar celălalt tip de scriere secretă constă din substituirea reciprocă doar a unui număr de litere-sunete, restul rămînînd neschimbate. De exemplu :

a k c t n m r e y
k a ſ p n n ſ s s
a este k, iar k este a etc.

În afară de aceste tipuri de criptografie, India antică folosea limba aluzivă, o formă de cod, precum și comunicarea cu ajutorul degetelor de la mînă, în care falangele substituiau consoanele, iar încheieturile vocalele.

A patra mare civilizație a antichității, cea din Mesopotamia, a atins, în criptografie, un nivel surprinzător pentru acele vremuri. Cea mai veche codificare este cuprinsă într-o tabletă de 7,5 x 5 cm și datează din anul 1 500 î.e.n.

Tableta conține cea mai veche formulă de fabricare a smalțului pentru vasele de lut. Scribul a folosit cuneiformele care aveau mai multe valori silabice, în sensul cel mai rar întâlnit. De asemenea, scribul a trunchiat sunetele, renunțînd la consoa-

nele finale ale unor semne silabice și a scris același cuvânt cu cuneiforme diferite în cadrul unui singur text.

Spre sfârșitul civilizației mesopotamice, scribii au început să semneze înlocuind cuneiformele-silabe ale propriilor nume cu cifre. Cu timpul, diferite cuneiforme-silabe, cele foarte des uzitate, au început să fie substituite cu cifre chiar și în interiorul cuvintelor și asta nu pentru a ascunde înțelesul celor scrise, ci pentru a epata și a atrage atenția. Aceste tablete au fost foarte ușor descifrate de către asiriologi. Asiriologul englez Erle Leichty a descifrat mai multe scrieri de acest gen și tot el a presupus că două tablete descoperite la Susa (în Iranul de astăzi) pot fi coduri. Pe bucățile de argilă spartă se găsesc două coloane paralele, una conținând cuneiforme reprezentând numere în ordine crescândă, iar cealaltă cuneiforme reprezentând sunete. Din nefericire, pe fragmentele de argilă recuperate nu se găsesc și numere folosite în textele cifrate descoperite până în prezent. Dacă aceste bucăți de argilă au fost într-adevăr coduri, atunci sint cele mai vechi coduri cunoscute din istoria omenirii.

Cultura ebraică a consemnat trei tipuri de transformare prin substituție. Astfel, în Vechiul Testament apare cuvântul Sheshach în locul cuvântului Babilon și Leb Kamai în loc de ~~Caldeeni~~.

Ambele transformări au rezultat din aplicarea unei substituții tradiționale de litere, în care prima literă a alfabetului ebraic era substituită cu ultima și viceversa, penultima o înlocuiește pe cea de a doua etc. De exemplu: $a = z$, $b = y$, $c = x$; ... $z = a$. Acest sistem de substituție se numea „atbash”.

Un alt sistem tradițional de substituție este cel numit „albam” și constă din împărțirea în două a alfabetului ebraic și substituirea reciprocă a literelor. Astfel, prima literă din partea întâi a alfabetului era substituită cu prima literă din partea a doua a alfabetului și așa mai departe.

Se cunoaște și un al treilea sistem de substituție, mai complicat, în care literele sint înlocuite cu cifre. Acest sistem s-a numit „atbabbh” și constă din substituirea primelor nouă litere

cu cifre de la unu la nouă, în așa fel încît suma rezultată din adunarea cifrei înlocuitoare cu numărul care reprezenta locul literei în alfabet să fie zece. Așa se înlocuia prima literă cu nouă, a doua cu opt etc., iar restul literelor se înlocuiau cu cifre care, adunate cu numărul de ordine al literelor, dădeau rezultatul o sută. Acest sistem era însă foarte confuz datorită modului de organizare a alfabetului ebraic și a numerelor ebraice.

Homer povestește pentru prima oară de folosirea conștientă a scrierii secrete în Grecia antică reproducînd legenda lui Bellerophon. Antela, soția regelui Proteus, s-a îndrăgostit de Bellerophon, dar acesta nu a plăcut-o. Regina, rănită în amorul propriu, s-a dus la rege și l-a mințit că Bellerophon a vrut să o siluiască. Infuriat, Proteus l-a trimis pe Bellerophon cu o scrisoare la regele Liciei, cerîndu-i acestuia să-l omoare, dar Bellerophon, prin faptele sale, cîștigă respectul regelui lician, care îi dă jumătate din regat și fata de soție.

Homer nu ne spune cum a fost scrisă această scrisoare de nu a putut fi citită de Bellerophon, preferînd să creeze în jurul ei o atmosferă de mister.

Cîteva secole mai tîrziu, Herodot, în ale sale „Istории”, se ocupă special de cîteva metode de steganografie (nu încă criptografie). Astfel, povestește că un med bogat, vrînd să se răzbune pe regele său, care-l făcuse să-și mînințe propriul copil, a trimis o scrisoare cu informații secrete, ascunse în burta unui iepure vînat în pădure, regelui Persiei, Cyrus, ajutîndu-l pe acesta să cucerească Mezia.

Tot Herodot povestește că un nobil persan a transmis gînerului său Aristagoras, din Milet, într-un mod bizar, un mesaj în care îl indemna la revoltă. Astfel, el a ras un sclav, a scris pe pielea capului lui informațiile pe care le aștepta Aristagoras, l-a lăsat să-i crească părul, apoi l-a trimis în Milet.

Conform cu „Istoriile” lui Herodot, spartanii au fost informați că Xerxes voia să cucerească Grecia de către un grec din Persia, care a transmis informații pe o placă de lemn acoperită cu ceară.

Spartanii au fost primii care au stabilit un sistem de criptografie militară. Încă din secolul al V-lea î.e.n., ei foloseau „skytala”, primul „mijloc tehnic” folosit în criptografie. Skytala era o bucată de lemn în jurul căreia se înfășura o fișie de papirus, piele sau pergament și apoi se scria mesajul de-a lungul bucății de lemn. Când se desfășura papirusul de pe skytală, apăreau o serie de litere dispersate, care nu aveau nici un sens, dar care, dacă materialul pe care se scrisese se înfășura pe o skytală de aceeași grosime, puteau fi citite.

Grecii au avut și alte realizări în domeniul criptografiei. Lumea datorează primele instrucțiuni privind securitatea comunicațiilor tot grecilor. Aceste instrucțiuni sînt cuprinse într-un capitol special din lucrarea lui Aeneas Tacticianul „Despre apărarea orașelor întărite”. Pe lângă instrucțiuni, se descriu și unele sisteme de cifrare. Astfel, într-un asemenea sistem se propunea înlocuirea vocalelor din textul clar cu puncte, iar consoanele rămineau neschimbate. Se recomanda, de asemenea, folosirea unui disc, în care se găseau anumite găuri reprezentînd literele alfabetului grecesc. „Cifrorul” trebuia să treacă un fir de ață prin literele care constituiau mesajul. „Descifrarea” se făcea prin procesul invers, iar semnificația mesajului apărea de-abia în momentul în care se termina scoaterea firului de ață din găurile discului. Un alt sistem sugerat de Aeneas a fost folosit și de spionii germani din primul război mondial și, cu o mică modificare, și în cel de-al doilea război mondial. Este vorba de a însemna, printr-o înțepătură, literele care constituie mesajul secret dintr-o scrisoare, carte sau alt document scris. Germanii, în cel de-al doilea război mondial, foloseau cerneala simpată pentru a însemna literele care formau mesajul secret.

Un alt grec, Polybius, a inventat un sistem de semnalizare care a fost ulterior adoptat pe scară largă ca metodă criptografică. El a aranjat literele alfabetului într-un pătrat și a numerotat rîndurile și coloanele.

În acest caz, fiecare literă putea fi reprezentată de două cifre — una care indica rîndul, iar cealaltă coloana în care se găsea litera respectivă. Polybius propunea ca aceste numere să fie transmise cu ajutorul torțelor — o torță în mina dreaptă

și cinci în mina stîngă însemnau litera e etc. Criptografii moderni au găsit câteva caracteristici patratului lui Polybius, sau careului cum i se spune acum, și anume: conversiunea literelor în numere și divizarea unei unități în două părți manevrabile. Careul lui Polybius, pe care îl prezentăm mai jos, a fost foarte mult folosit drept bază pentru un număr extrem de mare de sisteme de cifru.

	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	i	k
3	l	m	n	o	p
4	q	r	s	t	u
5	v	w	x	y	z

Cu toate acestea, nu se cunoaște dacă grecii au folosit pe scară mare cifrurile pe bază de substituție. Primele atestări despre folosirea lor sînt cuprinse în „Războaiele galice”, lucrarea lui Iulius Cezar, unde se prezintă modul în care a fost transmis un mesaj, scris cu litere grecești, lui Cicero, aflat într-o cetate asediată.

Suetonius scrie că Cezar folosea un cifru în care fiecare literă din textul clar era înlocuită cu o literă decalată cu trei locuri, după următorul model:

text clar — a b c d e f g h i j k l m n o p q r s t u v w x y z
 cifru — D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

După acest sistem, orice alfabet de cifrare care conține o periodicitate standard se numește alfabet Cezar.

Din lucrările de istorie rezultă că scrierile secrete se foloseau destul de mult de către romani și se spune că un gramatician, Valerius Probus, a scris chiar un tratat despre scrierile secrete ale lui Cezar, dar, din păcate, cartea s-a pierdut.

Se pare că, oriunde cultura a atins un anumit nivel de dezvoltare, în mod spontan a apărut și criptografia. Multiple nevoi i-au determinat pe oameni să recurgă la scrierile ascunse. Ast-

fel, Yezidi, o sectă obscură din nordul Irakului, folosea, de teama represaliilor musulmanilor, scrierea secretă când își redacta cărțile sfinte. Diferite sisteme de substituție se găsesc în vechile culturi din Tailanda, Malaya, Nigeria și chiar în unele insule din Pacific.

În Europa, rune teutone și oghamele celtice erau uneori

[illegibil]

Toate sistemele de criptografie runică se bazau pe înlocuirea literelor prin semne ce indicau numărul grupului literei și numărul literei în cadrul grupului.

Oghamele s-au păstrat mai ales pe inscripțiile de pe pietre funerare. Alfabetul acestor scrieri era format din cinci grupe de câte cinci litere, reprezentate de una pînă la cinci linii pornind de la o linie orizontală. Pentru primul grup, liniile erau situate deasupra orizontalei, pentru al doilea dedesubtul acesteia, pentru al treilea perpendicular, pentru al patrulea oblic, iar al cincilea eterogen.

Metodele acestea de criptare sînt catalogate într-o compilație, „Cartea lui Ballymote”.

O dată cu căderea Imperiului Roman, Europa alfabetului latin s-a prăbușit în întunericul Evului Mediu. Pămîntul pe care avea să se nască criptografia modernă uita arta și știința, iar din criptografie doar iscălitura anagramată a cîte unul călugăr plictisit mai pîlpiia ca o candelă în altarul bisericii, mai mult subliniind întunericul decît luminînd. În Evul Mediu, sistemele folosite pentru scrierea secretă erau foarte simple: cuvintele se scriau vertical sau de la coadă; în loc de vocale se puneau puncte, se foloseau alfabetele străine (grec, ebraic și armean) etc. Aproape o mie de ani criptologia civilizației apusene a stagnat.

Singurul om din Evul Mediu care a vorbit de criptografie, pe lângă faptul că s-a folosit de ea, a fost Roger Bacon, iar cel mai vestit cărturar care a avut cunoștință de criptografie în acele vremuri a fost un vameș englez, astronom amator și scriitor de geniu, pe nume Geoffrey Chaucer. Într-o lucrare de astronomie „Tratatul despre astrologie”, Chaucer include șase

pasaje criptate. Chaucer a substituit literele cu diferite semne făcute de el, punînd astfel bazele unui nou tip de scriere secretă.

În perioada aceasta însă, criptografia a căpătat o tentă de mister, fiind considerată o artă neagră, diavolească.

Scrierea secretă la arabi a apărut o dată cu interesul pentru literatură și gramatică, pentru rebus, epigrame, anagrame, ghicitori.

În anul 855, învățatul arab Abu Bakr Ahmad ben Ali ben Wahahiyya an-Nabati a inclus cîteva cifruri folosite de magie în cartea sa, „Cartea devotatului credincios care vrea să afle misterele scripturilor vechi”. Apoi, criptografia a căpătat și o altă întrebuintare. Astfel, într-un manuscris despre arta militară se vorbește de un cifru cu ajutorul căruia se relata despre compoziția materialului inflamabil ce era aruncat în cetățile asediate. Sectele religioase extremiste cultivau criptografia ca un mijloc de ascundere a părerilor lor față de credincioșii ortodocși.

Statele arabe au folosit, totuși, puțin cifrurile și codurile, deși în istoria lui Abd al-Rahman Ibn Khaldun se spune că funcționarii fiseului și cei din birourile armatei foloseau în relațiile dintre ei un cod special. Astfel, literele alfabetului sau numele de oameni erau înlocuite cu nume de parfumuri, fructe, păsări, flori ori alte semne decît cele general cunoscute.

Cunoștințele arabilor în domeniul criptologiei au fost concentrate într-o secțiune specială a enciclopediei în 14 volume „Subh al-asha”. Secțiunea despre criptologie intitulată „Cu privire la ascunderea mesajelor secrete în scrisori” are două părți, prima referindu-se la sisteme simbolice și aluzive, iar cealaltă la cerneluri simpatice și criptologie propriu-zisă.

Autorul acestei enciclopedii, Qualqashandi, își datorează informațiile scrierilor sale lui Ibn ad-Durailim. Qualqashandi începe secțiunea despre criptologie explicînd de ce uneori este necesar să se asigure secretul unor mesaje și, după ce arată că se poate asigura secretul unor informații folosindu-se o limbă străină puțin cunoscută, el dă șapte sisteme de criptare :

1) O literă se înlocuiește cu alta; 2) criptologul poate scrie cuvântul invers, de la coadă; 3) se poate schimba locul literelor din cuvintele care alcătuiesc mesajul; 4) se pot da literelor valorile lor numerice, după sistemul în care literele arabe sînt folosite ca cifre, scriind astfel cuvântul cu ajutorul numerelor; 5) se poate înlocui fiecare literă a textului clar cu două litere a căror valoare numerică adunată să dea o sumă egală cu valoarea numerică a literei substituite; 6) fiecare literă poate fi substituită cu un nume de persoană sau ceva asemănător; 7) se pot folosi nume de țări, fenomene cosmice, nume de fructe, flori, copaci pentru a substitui literele sau să se deseneze păsări sau alte ființe ori, pur și simplu, să se inventeze simboluri speciale cu care să se înlocuiască literele.

Această listă cuprinde atît sisteme bazate pe substituție, cît și pe transpoziție, iar sistemul „5” preconizează, pentru prima dată, folosirea mai multor elemente pentru substituirea unei litere.

Filologii arabi, mai ales gramaticienii din Basra, Kufa și Bagdad, prin studierea Coranului au încercat, numărînd frecvența cuvintelor, să stabilească ordinea cronologică a versetelor din Coran.

Cu această ocazie, ei au observat că unele cuvinte au fost folosite mai des doar în ultima parte a acestuia și le-au examinat din punct de vedere fonetic să vadă dacă erau arabe sau împrumuturi. Toate aceste studii au dus la generalizări despre compoziția cuvintelor arabe și astfel s-a ajuns la concluzia că sînt foarte puține cuvinte, formate din mai mult de cinci litere, care să nu cuprindă lingualele *r*, *l* și *n* sau labialele *f*, *b* și *m*.

De asemenea, de mare importanță pentru criptanaliză au fost descoperirile făcute cu ocazia întocmirii de dicționare sau, mai bine-zis, a dezvoltării lexicografiei.

Cînd întocmește un dicționar, lingvistul se lovește întotdeauna de problema frecvenței literelor și a asocierilor de litere. Astfel, arabii au aflat foarte repede că cel mai rar întîlnit în arabă este litera *z*, iar cel mai des întîlnite sînt literele care alcătuiesc articolul hotărît al, adică *a* și *l*. Se înțelege, deci,

de ce primul mare filolog al lumii, Al-Khalil, a scris o carte numită „Manualul limbii secrete”. Lucrarea i-a fost inspirată de modul în care a reușit să găsească soluția unei criptograme scrisă în limba greacă și care îi fusese trimisă pentru decriptare de către împăratul bizantin.

Întrebat cum a reușit să decripteze scrisoarea, Al-Khalil a afirmat că primul lui gînd a fost că mesajul respectiv trebuia să înceapă cu „În numele lui Dumnezeu” sau ceva asemănător. Foarte curînd, prezumția lui s-a dovedit justă.

Această afirmație, precum și faptul că lui Al-Khalil i-a trebuit o lună să decripteze scrisoarea demonstrează că arabii nu formulaseră încă cele mai analitice tehnici ale criptanalizei, bazate pe frecvența literelor. Dar 600 de ani mai tîrziu, studiile lingvistice au ajutat un necunoscut să aplice observațiile făcute și în criptanaliză, căci Qualqashandi scrie că: „Ocazional, secretari pricepuți, deși nu cunosc codul, totuși cunosc reguli care îi ajută, prin combinații, să rezolve enigme”.

Qualqashandi vorbește, în continuare, despre modul în care se face criptanaliza unui text, făcînd inițial afirmația că orice criptanalist trebuie să știe în ce limbă e scris mesajul de decriptat. Afirînd că araba este limba cel mai des folosită, îi descrie foarte amănunțit caracteristicile. Se dă, astfel, lista literelor care nu se întîlnesc niciodată împreună într-un cuvînt, a literelor care intră foarte rar în combinații sau combinații de litere care nu sînt posibile. Urmează apoi lista literelor în ordinea frecvenței lor din versetele Coranului, făcîndu-se mențiunea că în alte texte frecvența poate fi diferită. După ce a făcut toate aceste precizări, Qualqashandi a scris :

„Cînd doriți să găsiți soluția unui mesaj cifrat, începeți prin a-i număra literele, apoi numărați de cîte ori se repetă fiecare simbol în parte, notîndu-vă rezultatele. Dacă persoana care a scris mesajul a fost atît de vicleană încît a ascuns despărțirea cuvintelor între ele printr-un simbol, primul lucru care trebuie să-l faceți este să-l identificați pe acesta. În acest scop luați al doilea simbol din mesaj și considerați-l ca fiind semnul de despărțire, apoi căutați-l în tot mesajul, observînd dacă combinațiile celorlalte semne ar putea forma cuvinte, ținîndu-se seama

în contact și cîte dintre acestea sînt diferite). Frecvența cripto-
gramei de mai sus este următoarea :

17	4	13	0	7	17	23	26	5	12	3	2	2
A	B	C	D	E	F	G	H	I	J	K	L	M
36	25	1	5	0	0	23	20	3	6	9	13	8
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Un tabel al frecvenței într-un text în engleză (baza-
ră pe 100 de litere ar putea fi următorul)

	16	3	6	8	21	4	7	12	13	1	1	7	6
	A	B	C	D	E	F	G	H	I	J	K	L	M
Frecvența)	8	15	4	4	13	2	15	6	6	5	0	5	3
	14	16	4	1	13	12	13	6	2	3	1	4	1
	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Procentaj	7	8	2	0,25	6	6	9	3	1	1	5	0,5	2

Dar nu este posibil să facem substituirea luînd, în mod
mecanic, literele din criptogramă, în ordinea frecvenței și ală-
turîndu-le listei cu frecvența într-un text obișnuit.

În cazul nostru, cele două liste ar apărea așa :

text obișnuit	e	t	a	o	n	i	r	s	h	d	l	u	c	m
criptograma	N	H	O	G	T	U	A	F	C	Y	J	X	Z	E
text obișnuit	p	f	y	w	g	b	v	j	k	q	x	z		
criptograma	W	I	Q	B	X	V	L	M	P					

Substituția mecanică a celor două texte ar da un text de
tipul următor : N H O G T U A F C Y J X Z E W I Q B X V L M P
Nu trebuie să
se surprindă pe cineva de acest lucru, deoarece cele două liste sînt
între ele diferite, cuprîndînd ca întotdeauna diferite, formate
din altele diferite. Totuși frecvența lor se schimbă foarte puțin.
Mendipa unde se găsea mult de locuri obișnuit de pe lista
frecvenței. Căci text ar fi literele e, t, a, o, n, i, r, s și h vor
forma grupuri de litere cel mai des întâlnite, urmează apoi
grupul literelor d, l, u, c și m. Întotdeauna destul de frecvent, grupul

literelor p, f, y, w, g, b găsite mai rar și ultimul grup, cel al
literelor j, k, q, x și z, care se întîlnesc foarte rar.

Dacă un criptanalist a reușit să identifice, într-un fel sau
altul, unele litere dintr-un text cifrat, celălalte le descoperă
ghicindu-le, ca în textul de mai jos :

G I X X N G G O T Z N U C O T W M O H

e i n e a i n i t

Y J T K T A M T X O B Y N F G O G I N U G J E N

h a n o n i h e i c a e

Z V Q H Y N G N E A J F H Y O T W G O T H Y N A F Z

t h e e o t h i n i n t h e o

N F T U I N Z A N F G N L N F U T X N X U F N E J C I N H Y A

e n a c o e e e a n e a e e t h o

Z G A E

o

U T I C Q G O G O T H J O H O A T C J N K H Y N I V O C O H Q I H

a n a i i n t i t i o n t h e a i i t a t

C N U G H H A F N U Z H Y

e a t t o e a t h

Aproape de începutul textului se găsește combinația *ith*.
Acele litere pot face parte din cuvîntul *with*.

Nici un criptanalist, dacă ar fi întrebă, n-ar avea cum să
vă dovedească că presupunerea lui e corectă. De acum încolo
total se rezumă la ghicit, operațiune ghidată doar de elasticile
legi ale probabilității. Presupunerile succesive vor confirma su-
porții le inițiale sau le vor infirma, deși fiecare presupunere
pornește de la aceeași bază extrem de șubredă. În cele din urmă
însa, consistența rezultatului final este atît de probabilă încît
validitatea soluției devine certitudine. Se știe că criptanalistul
care caută dovezi absolute pentru fiecare presupunere pe care
o face nu va găsi niciodată soluția unei cripto-grame. Dar să re-
venim. În cazul nostru se pare că *with* este cuvîntul care se

ascundă sub aceste litere, ceea ce ar însemna că M — W. Se face încercarea lui în criptogramă cu scopul de a vedea dacă nu ceva nu ne sugerează și alte cuvinte. Zece litere în con-
ținute formează șevrea with unknown — care ne duce la
deducția că ar putea fi vorba de expresia with unknown. Șe-
vra din text este — unknown — iar de preluatul și verificării
cuvintelor se vede că așa este. Cuvintele apare cuvintele
unknown și with litera care are ca apăsări sunt marcate în text
ca fiind cele care trebuie să fie găsite. Acest proces de re-
construcție a textului, care pe lângă el mai are și o lă-
muri amuzant din criptanaliză, este numit „anagramare”. El
poate fi accelerat de o reconstrucție paralelă și anume aceea a
cheii de cifrare. Dacă literele din textul cifrat sînt scrise sub
un alfabet normal, acest aranjament ne furnizează, de multe ori,
și alți echivalenți. În cazul de față, situația se prezintă astfel :

Alfabet clar a b c d e f g h i j k l m n o p q r s t u v w x y z
Alfabet cifrat u n y o k t a h j m

[illegible]

Alfabet clar a b c d e f g h i j k l m n o p q r s t u v w x y z
Alfabet cifrat CHIMPANZEBDFGJKLOQRSTUUVWXY

Partea a doua a alfabetului este alfabetul care apare după eliminarea
unor litere din alfabetul anterior. Uneori, criptanalistul
poate descoperi unele secvențe care au fost parțial descip-
tate din cauza unei erori și alți echivalenți. De exemplu, dacă
secvența $QR - TU$, nu-i nevoie de prea mult efort
pentru a ști de seamă că litera care lipsește este s . Asemenea
secvențe sar în ochi în cazul alfabetului parțial descipat din

criptogramă $HJ - M$. Dacă două litere pot să intre în acest spațiu K și L . Dar k a fost identificat în cuvântul *unknown*, dec. $L = V$. Același lucru îl poate ajuta pe criptanalist să verifice dacă F și G sunt r și s . Dacă $F = s$ și $G = r$, ordinea în alfabet ar apărea ca sr , dec. nu e bine și acum știm sigur că $F = r$ și $G = s$. Alfabetul de cifrat ne asigură, de asemenea, și o serie de indicii pentru echivalența din textul clar. Așa, de exemplu, $u = a$ în alfabet. Deci, în cazul în care criptanalistul observă un V în criptogramă, el încearcă să vadă dacă V nu este cumva b și aceasta datorită secvențelor UV și ab . În cazul de față, această presupunere se dovedește justă. Cu noile descoperiri, inserate în primele două rânduri, soluția, putem spune fără frică, a fost găsită :

G J X X N G G O T Z N U C O T W M O H
s u e s s i n e a i n w i t
Y J T K T A M T X O B Y N F G O G I N U G
h u n k n o w n i h e r s i s e a s
J F N Z V Q H Y N G N E A J F H Y O T W
u r e b t h e s e c o u r t h i n

Cei doi *XX* pot fi cei doi *cc* din *success*, apoi *B* trebuie să fie *p* din *ciphers*; *E* trebuie să fie *f* din *four*; *W* = *g* din *things* sau din *-ing* și așa mai departe. Textul clar, inserind și semnele de punctuație, ar fi :

„Success in dealing with unknown ciphers is measured by the four things in order named: perseverance, careful methods of analysis, intuition, luck. The ability at least to read the language of the original text is very desirable but not essential" 1.

În situația de față, cheia folosită la cifrare a fost NEW YORK CITY.

* În limba română: „Sucesul în rezolvarea cifrelor necunoscute este asigurat de următoarele patru lucruri enumerate în ordine: perseverență, muncă de bună calitate, răbdare și încredere în propriile forțe. În limba în care este scris textul original e de dorit într-un grad foarte înalt, dar nu ~~este~~ esențială

În cazul scrierilor mai vechi, de multe ori soluția se poate afla doar din cunoașterea caracteristicilor și articulelor, cum ar fi: "a" care apare de multe ori și se repetă mai des decât "b", "c" care apare de multe ori și se repetă mai des decât "d", "e" care apare de multe ori și se repetă mai des decât "f", "g" care apare de multe ori și se repetă mai des decât "h", "i" care apare de multe ori și se repetă mai des decât "j", "k" care apare de multe ori și se repetă mai des decât "l", "m" care apare de multe ori și se repetă mai des decât "n", "o" care apare de multe ori și se repetă mai des decât "p", "q" care apare de multe ori și se repetă mai des decât "r", "s" care apare de multe ori și se repetă mai des decât "t", "u" care apare de multe ori și se repetă mai des decât "v", "w" care apare de multe ori și se repetă mai des decât "x", "y" care apare de multe ori și se repetă mai des decât "z". Această cunoaștere a caracteristicilor textului clar stă la baza soluționării unor cifruri și coduri mult mai complexe. Natural, soluția criptogramelor scurte este mult mai greu de găsit decât a celor lungi, care conțin multe cuvinte și fraze complete.

Pentru problemele mai dificile, experții sfătuiesc pe novici: 1) cînd nu este evident niciun fel de caracteristică, să se încerce să se găsească o soluție prin încercare; 2) cînd nu este evident niciun fel de caracteristică, să se încerce să se găsească o soluție prin încercare; 3) cînd nu este evident niciun fel de caracteristică, să se încerce să se găsească o soluție prin încercare; 4) cînd nu este evident niciun fel de caracteristică, să se încerce să se găsească o soluție prin încercare; 5) cînd nu este evident niciun fel de caracteristică, să se încerce să se găsească o soluție prin încercare; 6) cînd nu este evident niciun fel de caracteristică, să se încerce să se găsească o soluție prin încercare; 7) cînd nu este evident niciun fel de caracteristică, să se încerce să se găsească o soluție prin încercare; 8) cînd nu este evident niciun fel de caracteristică, să se încerce să se găsească o soluție prin încercare; 9) cînd nu este evident niciun fel de caracteristică, să se încerce să se găsească o soluție prin încercare; 10) cînd nu este evident niciun fel de caracteristică, să se încerce să se găsească o soluție prin încercare.

RIDICAREA VESTULUI

De la începutul secolului al XVIII-lea, Europa apăsătoare a început să folosească criptografa în documentele oficiale și personale, dar și în scrisorile din acea vreme erau în mare măsură criptate. De atunci toate celelalte elemente ale criptografiei care peste secole vor domina lumea. Sistemul de criptare în scrisorile secrete era foarte complicat și chiar și în zilele noastre pe alături de mai multe și mai noi, influența primei criptografii, începând cu secolul al XVIII-lea, nu a mai rămas neobservată, ci s-a dezvoltat continuu sub cele două forme de bază cunoscute și astăzi: coduri și cifruri.

Substituițiile în coduri și au originea altă în acronimele și în epitetul și figurile de stil folosite de oracole și vrăjitori. (Formele magice marcate pe jumătate sa sublinieze, pe jumătate să se ascundă în cuvintele înțelese al vrăjitorilor)

Cel mai vechi document criptografic aflat în arhivele Vaticanului este un document substituit, provenind din ambele secole. Este vorba de o literă pe care sunt trecuți guelfii care-l susțineau pe papă și ghibelina care-l susțineau pe împăratul german. În acest document, guelfii erau numiți "egipteni", iar ghibelina "cepii din Israel". Mai târziu, după vreo zece ani, pe o bucată de hârtie a fost scris primul cod modern. În acest cod, bazat pe substituție, o literă ține locul unui cuvânt. Astfel: a = rege, d = papa, s = Marescallus și așa mai departe.

În ce privește cifrurile, acestea au fost folosite destul de des. Astfel, vocalele erau înlocuite cu puncte sau cruce. Astfel:

către Olanda, demonstrând lumii importanța criptologiei în făurirea istoriei.

Printre cei mai buni criptologi ai timpului se numărau mai ales cei care lucrau pentru papa. În serviciul papei s-a înființat chiar un post de secretar-cifror. După 1580, acest post a intrat în posesia unei familii de criptologi care au impulsinat dezvoltarea criptologiei în ansamblul ei.

Este vorba de familia Argenti. Giovanni Batista Argenti a intrat în serviciul papal ca secretar al lui Antonio Elia, care l-a învățat meseria de criptolog. Nepotul lui Giovanni Argenti, Matteo Argenti, a învățat și el criptologie. El a făcut chiar și un manual de criptologie, în care a concentrat tot ceea ce realizase mai bun Renașterea în acest domeniu.

Cei din familia Argenti au fost primii care au folosit un cuvânt drept cheie pentru întocmirea unor alfabete cifrate. Procedeu este următorul: se scrie cheia, omițându-se literele care se repetă, apoi se completează șirul de litere cu restul alfabetului după modelul de mai jos:

P I E T R O a b c d e f g h i l m n o p q r s u z
10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29

Cunoscând că secvența *qu* din textele clare este invariabilă și că *u* are o formă simbolică litere, Argenti a substituit-o cu *qu* în textul cifrat. De asemenea, din cauza rarității literei *q* din alfabetul italian, art corbani, în textul cifrat s-a înlocuit-o una dintre acestea. Astfel, în loc de *sigillo* din textul clar, în textul cifrat se scria *sigilo*. Pentru a îngreua descifrarea, el, Matteo Argenti, folosea numere de la 3 la E pe un rând.

El menționa despărțirea în cuvinte, punctuația și accentuile, care prin asta se făceau în clar, ceea ce confera textului cifrat o rezistență superioară.

În același timp, foloseau atât numere formate dintr-o singură cifră cât și numere formate din două cifre, având grijă ca numerele compuse dintr-o singură cifră să înlocuiască litere

cu frecvență mare, pentru a nu atrage atenția prin raritatea lor. Iată un astfel de cifru folosit de Matteo Argenti:

a b c d e f g h i l m n o p q r s t u z
1 86 02 20 62 22 06 60 3 24 26 84 9 66 68 28 42 80 04 88

et con non che nub

08 64 00 44 57

Foloseau, de asemenea, foarte mult polifonele — simboluri care aveau două sau chiar trei înțelesuri — alese însă în așa fel încât să nu îngreueze decriptarea de către destinatar. Matteo Argenti folosea, de asemenea, cifruri pe care le adapta în funcție de alfabetul limbii în care era scris textul de cifrat, neavind un cifru standard, universal valabil pentru toate limbile.

Toate aceste succese duceau la nașterea unei științe evoluată, în conformitate cu progresul realizat de cunoașterea umană.

Părintele criptologiei apusene a fost Leon Battista Alberti, primul dintr-un grup de oameni care au inventat, element după element, un sistem de cifru cărui li aparțin majoritatea cifrurilor folosite astăzi. Este vorba de substituția polialfabetică. După cum arată și numele, avem de-a face cu două sau mai multe alfabete-cifru. Deoarece mai multe alfabete folosesc aceleași simboluri (în special litere) pentru cifrare, un anumit simbol poate reprezenta diferite litere din același text clar, în funcție de alfabetul care a fost folosit. În mod sigur, acest lucru îl va dezorienta pe criptanalist. Se poate întâmpla însă ca și criptograful să facă anumite confuzii, nemaștiind care alfabet a fost folosit și, pentru a se evita acest lucru, se stabilesc anumite reguli și convenții.

Apariția substituției polialfabetice a însemnat un uriaș pas înainte în criptologie, dar a fost nevoie de peste 400 de ani până când aceasta s-a impus în criptografia politică. În secolul XX, folosirea ei a atins un înalt grad de complexitate, ceea ce asigură textelor cifrate o rezistență extraordinară.

Cei care au inventat acest sistem de cifrare au fost amatori, deoarece profesioniștii, care li întreceau pe amatori în criptanaliză, se concentrau asupra problemelor curente și asupra sistemelor care se foloseau pe vremea aceea, dar care astăzi sunt depășite. Amatori, nelegăți de astfel de probleme făceau mai mult teorie, mai idene a patru asemenea amatori — un arhitect, un cleric, un curtean și un naturalist — au prins aripă.

Arhitectul a fost Alberti, care, la fel ca și Leonardo da Vinci, intruchipa omul universal al Renașterii. La rugămintea secretarului pontifical Leonardo Dato, Alberti a studiat și a scris un eseu despre criptologie. După ce a reconstituit modul de descifrare a textelor criptate, a trecut la căutarea unor procedee de criptare care să reziste criptanaliștilor. Apoi a analizat pe rând diferitele sisteme de cifrare: substituții, transpoziții de litere, punctarea literelor care constituiau un mesaj secret ascuns în interiorul unei scrisori, folosirea cernețurilor simplice etc. În eseuul său a prezentat și un cifru făcut de el, despre care, la fel ca toți criptologii, spunea că nu poate fi spart. Este vorba de discul de cifrat, care a ajutat la fundamentarea polialfabetismului. Cu această invenție, Occidentul a preluat hegemonia lumii în probleme de criptologie și n-a mai cedat-o niciodată.

Acum să-l dăm cuvintul lui Alberti pentru a-și prezenta invenția:

„Am făcut două discuri rotunde din plăci de aramă. Pe cel mai mic am scris stator, iar pe cel mai mare rotor. Diametrul statorului este de 19 mm, în timp ce al rotorului. Apoi am împărțit fiecare disc în 24 de părți egale și spațiile rezultate am numărat cu cifre. În celulele discului mai mare am scris alfabetul latin cu excepția literelor H, K și Y, deoarece ele nu sunt necesare. Asta a însemnat 20 de litere, deoarece J, U și W nu făceau parte din alfabetul conceput de mine. În spațiile goale am scris cifrele 1, 2, 3 și 4. În fiecare din cele 24 celule ale rotorului am scris o literă mică, dar nu în ordine alfabetică, cum este cazul cu statorul, ci la întâmplare

Toate cele 24 de celule au fost umplute, deoarece alfabetul latin are 24 de litere, printre care și et. După ce am făcut completările respective, am așezat rotorul peste stator, iar prin centru am înfipt un ac pe care se învârtea rotorul”.

Procedeeul de lucru este următorul. Corespondenții trebuie să aibă discuri identice și să cadă de acord asupra unei litere index de pe rotor. Ca să execute cifrarea, expeditorul fixează această literă în dreptul oricărei litere de pe stator, având încă grijă ca aceasta să apară prima în textul cifrat. Alberti dă exemplul cu litera K în dreptul lui B. După aceasta, toate literele de pe rotor, care formează cuvintele din mesaj, sunt înlocuite cu cele de pe stator, aflate în dreptul lor. Până aici nimic deosebit, dar cu următoarea frază Alberti a deschis drumul criptologiei moderne:

„După ce am cifrat trei sau patru cuvinte, schimb poziția indexului în dreptul lui d. Din acest moment, K nu mai este echivalent cu B, ci cu d, iar toate celelalte litere vor primi noi echivalenți”.

Fiecare nouă mișcare a rotorului înseamnă un nou cifru, în care atât literele textului clar cit și echivalenții lor sunt schimbați unul față de altul. În cazul de față, există exact atâtea cifruri câte poziții are discul. Discul lui Alberti a fost primul cifru polialfabetic din istoria criptologiei.

Acestei realizări, Alberti i-a adăugat o altă tot atât de remarcabilă: codul cifrat. Vorbind și de această invenție, avem explicația de ce Alberti a trecut pe discul exterior numerele de la 1 la 4. Într-un tabel, el a făcut permutări din aceste cifre, luate câte două, câte trei și câte patru, obținând 336 de numere, între 11 și 4444.

În tabelul respectiv, în dreptul fiecărei cifre, se trecea o frază, o expresie sau un cuvânt. De exemplu, în dreptul lui 12 se scria: „Am pregătit corăbule promise și trupele s-au imbarcat având și hrana necesară”. Aceste liste de cod nu se schimbau, dar cifrele rezultate în urma codificării erau cifrate cu ajutorul discului, ca și cum ar fi fost litere simple. Operația ducea la schimbarea reprezentării codificate. Astfel, 341 = pază era o dată mrp, iar altă dată fco. Această invenție a fost deose-

bit de valoare, dar au trecut 400 de ani până când marile puteri au început să o folosească

În 1518 la Würzburg, marele abatele mănăstirii, Johann Trithemius, o născut la 1462, care lăsa în urma lui un manuscris cu titlul „Poligrafia”. Urmasul său la conducerea mănăstirii a publicat lucrarea fiind astfel primul editor al unei lucrări de criptologie tipărite. Concepută din șase cărți, lucrarea cuprinde coloane de cuvinte tipărite în alfabetul gotic folosit de Trithemius în scrierile sale originale. În prima carte sunt 384 coloane de cuvinte latinești, cite două pe fiecare pagină cuprind, criptat, vestitul Ave Maria. Este cea mai cunoscută invenție a lui Trithemius. El a selectat în așa fel cuvintele, echivalenții literelor fiind luați din tabele consecutive, încât, în textul criptat, acestea au căpătat forma unei rugăciuni inocente. Astfel, cuvântul abate este criptat ca fiind deus clementissimus regius aevum infinet. Celelalte cărți cuprind sisteme de cifru asemănătoare, care, uneori, capătă o tentă de formule magice.

Cartea a cincea, însă, reprezintă contribuția adusă de abatele Trithemius la dezvoltarea polialfabetismului. În această carte apare pentru prima dată tabelul pătrat sau tabelul lui Trithemius, care este o matrice de 26 x 26 de litere, în care fiecare literă este combinată cu fiecare literă din alfabetul latin. Acest tabel este folosit pentru a cripta și decodifica textele folosind o cheie de cifru. Tabelul este prezentat în următoarea formă:

Tabelul lui Trithemius este o matrice de 26 x 26 de litere, în care fiecare literă este combinată cu fiecare literă din alfabetul latin. Acest tabel este folosit pentru a cripta și decodifica textele folosind o cheie de cifru. Tabelul este prezentat în următoarea formă:

cazul de față, el schimba alfabetul textului, dar după prima grupă de 24 de litere, dar de cele mai multe ori folosea același alfabet pentru tot textul

a b c d e f g h i j k l m n o p q r s t u x y z w
b c d e f g h i j k l m n o p q r s t u x y z w a
c d e f g h i j k l m n o p q r s t u x y z w a b
d e f g h i j k l m n o p q r s t u x y z w a b c
...
z w a b c d e f g h i j k l m n o p q r s t u x y
w a b c d e f g h i j k l m n o p q r s t u x y z

Marile avantaje față de invenția lui Alberti este acela că un nou alfabet de cifrat este folosit pentru fiecare literă. Alberti schimba alfabetul după fiecare patru litere, iar rezultatele păreau să dea în vîltag cuvinte de tipul lui papa sau atae, existînd șanse ca criptonalistul să descopere mecanismul și să dezbănească mecanismul criptogramelor. Noul sistem exclude această posibilitate.

Sistemul de cifrare elaborat de Trithemius este în același timp și primul exemplu de cheie progresivă, în care alfabetele folosite sînt scoase din uz înainte de a se fi repetat. Mașinile moderne de cifrat folosesc deseori asemenea chei, dar evită principalele defecte ale sistemului lui Trithemius, și anume: periodicitatea alfabetelor și ordinea rigidă a folosirii lor.

Trithemius a avut o influență deosebită în criptologie, datorită mai ales autorității pe care o conferă textul tipărit, iar tabloul său a devenit clasic pentru întreaga criptologie.

Dacă despre primul doi, care au contribuit la dezvoltarea criptografiei pe baza polialfabetismului, istoria ne furnizează date bogate, despre cel de-al treilea se știe doar că era nobil din Brescia, pe nume Giovan Batista Belaso, că a făcut parte din suita unui cardinal, iar în 1553 a publicat o cărțuie cu titlul „La cifra”. În această cărțuie, signor Giovan Batista Belaso propunea folosirea unei chei literare ușor de ținut minte și de schimbat pentru cifrurile polialfabetice. Belaso numea această cheie contrasemn și spunea că „poate fi formată din

cuvinte din limbile italice sau latine sau din orice altă limbă. Ea poate conține două sau mai multe cuvinte, după dorința fiecăruia. Luăm textul pe care dărim să-l cifrăm și-l punem pe hârtie scriind cuvintele nu prea aproape între ele. Apoi, deasupra fiecărei litere scriem o literă din contrasemnului ales de noi. Să luăm drept exemplu, cartul în care contrasemnului nostru a fost veretul Virtuti omnia parent și să spunem că ceea ce rezultăm să cifrăm este textul: Larmata Turchesca paria a ce que de Lado. Le vom scrie pe litere în felul următor:

V I R T U T I O M N I A P A R E N T V I
L a r m a t a T u r c h e s c a p a r i a a c e q u e d e L a d o

Litera din cheie indică alfabetul din tablou, care urmează să fie folosit pentru cifrarea literei clare. Astfel, I urmează să fie cifrat cu litera corespunzătoare din alfabetul V, o cu litera corespunzătoare din alfabetul L. Sistemul permite o mare flexibilitate, nemaifiind nevoie ca toate mesajele să fie cifrate cu unul din cele relativ puține alfabete de cifrat.

Acest sistem a prins repede, iar invenția lui Belaso a pus în evidență că pentru a descifra un text, se folosesc mai multe chei, care se schimbă la intervale neregulate.

Belaso, ca și Trithemius, a folosit alfabete de cifrat standard, așa că a rămas în seama unui naturalist să reinvie alfabetul. Acesta a fost făcut de un naturalist, dar înveștă de trei, conceptul modern de substituție polialfabetică.

Naturalistul, primul care a trecut la cunoașterea naturii și a experimentat, a fost Leonardo da Vinci. El a fost unul din cei mai de seamă oameni de știință de pe timpul Renașterii.

În istoria criptologiei a rămas datat un carticel. În 1469, Leonardo da Vinci a scris pe o bucată de pergament:

Marea calitate a acestei lucrări este perspectiva pe care o oferă asupra lumii. Cu patru capitole în care se discută despre criptologia modernă, criptologia modernă este criptologia modernă.



analiza și prezintă o listă de particularități care ajută la soluționarea criptogramelor.

Printre cifrurile prezentate se întâlnește și primul cifru digrafic, în care două litere erau reprezentate de un singur simbol.

El clasifică metodele de cifrare în trei sisteme: 1) schimbarea ordinii literelor (transpoziția); 2) a formei literelor (substituție prin simbol); 3) a valorii literelor (substituție prin literă aparținând altui alfabet). Aceasta a fost prima clasificare a cifrurilor în cifruri de transpoziție și substituție.

El sfătuiește de asemenea, pe cifrari să folosească în textul clar și mai multe sinonime, iar unele cuvinte să fie ortografiate cu bună înțelegere, pentru a îngreuna soluționarea criptogramelor.

În carte sunt mai multe discursuri și este explicat modul în care acestea pot fi transformate în tablouri, descriind, de asemenea, și modul în care se poate soluționa un cifru monoalfabetic atunci când criptograma nu conține desparțirea în cuvinte sau când desparțirea este făcută arbitrar. Dar, poate cea mai de seamă contribuție a sa, pe această linie, este încercarea de a soluționa cifruri polialfabetice și de a pune la punct metoda cunoscută azi sub numele de metoda cuvintului probabil. Astfel, scoțind în relief care este diferența dintre această metodă și analiza lingvistică, spunea: „Când se cunoaște, în general, despre ce este vorba în mesaj, criptanalistul poate încerca să ghicească cuvintele din criptogramă, analizând fiecare cuvânt (număr de litere, ordinea și comparându-le cu supozițiile sale). În fiecare domeniu există un număr de cuvinte mai frecvente. Astfel, dacă este vorba de război, cuvinte ca soldat, comandant, general, tabără, armată, arme, a lupta etc. se întâlnesc foarte des. În felul acesta, se poate decripta un text, fără a se face analiza lingvistică a textului cifrat”.

Porta, adoptând singura poziție care asigură succesul în criptanaliză — a refuzat să creadă în invincibilitatea cifrurilor polialfabetice — a reușit să soluționeze câteva asemenea cifruri, reușită cu atât mai remarcabilă, cu cât această problemă

eta considerată de criptologia renascentistă ca fiind de nerezonabil.

Primul cifru polialfabetic pe care l-a soluționat și care a fost realizat cu ajutorul unui disc învârtit în sensul acelor ceasornicului, după cifrarea fiecărei litere, avea un caracter progresiv. Porta a observat că în cazul în care trei litere apar în ordine alfabetică, în cuvântul din textul clar (de exemplu, o f d n defici sau sta din studium) și discul se mișcă progresiv ca un singur spațiu. Astfel, în mod succesiv, în fața fiecăreia din cele trei litere va apărea același simbol, rezultând o repetare de trei ori a lui. Folosindu-se de această constatare, Porta a soluționat o criptogramă și a reconstruit alfabetul de cifrat. În cazul celei de-a doua soluții, Porta și-a schimbat metoda.

De data aceasta repetarea de trei ori a unui simbol i-a semnalizat faptul că fusese folosită o cheie care conținea un cuvânt având în compoziția sa trei litere așezate în ordine alfabetică. După ce a cifrat trei litere așezate în ordine inversă, a observat că rezultatul este identic. În timp ce se ocupa de această observație, a descoperit că dintr-un set de 51 de litere, într-un cuvânt de 17 litere apar toate cele trei litere repetate în cel de-al treisprezecelea cuvânt, am ajuns la concluzia că cheia se repetase de 17 ori. După ce a descoperit că din 17 litere a fost pe punctul de a descoperi metoda de decriptare a cifrurilor polialfabetice, dar el n-a dat atenție descoperirii sale și, mai mult de 300 de ani, cifrurile polialfabetice au fost considerate ca fiind inviolabile. Contribuția lui Porta la dezvoltarea criptologiei a rămas în mare măsură necunoscută datorită faptului că el n-a conceput niciun sistem mai avansat asupra sistemului polialfabetic.

Deși Porta reușise să închege un sistem de cifrare bazat pe cifrul polialfabetic, acesta nu se mai putea adăci în bucuria lui. Într-o scrisoare din anul 1568, el a scris că în secolul al XVI-lea au apărut mai multe metode de folosire a cheii lui Belaso și i-a adăugat perfecționări.

O cheie care se schimbă la fiecare mesaj asigură o rezistență mai mare decât una folosită de mai multe ori și de aceea, au început să se folosească chei pentru fiecare mesaj nou. Cu

doi au descoperit un mijloc foarte inteligent de a se asigura schimbarea cheii și anume folosirea chiar a textului clar drept cheie. Procedul s-a numit sistemul autocheie.

Inventatorul primului procedeu de folosire a autocheii, Cardano, un doctor și, în același timp, matematician milanez a rămas în criptografie mai mult datorită contribuției sale la dezvoltarea steganografiei, decât datorită noului procedeu. Modul în care a conceput el folosirea noului sistem este defectuos, așa că nu vom insista asupra lui.

Istoriografia criptologiei a dat dovadă de cea mai crasă eroare și neglijență în legătură cu inventatorul celui de-al doilea procedeu al autocheii. Astfel, a fost ignorată această contribuție esențială și s-a dat numele cunoscutului Blaise de Vigenere unui cifru elementar și primitiv, cu care el n-a avut nimic de-a face.

Vigenere nu era de origine nobilă, dar la vârsta de 24 de ani a intrat în slujba ducelui de Nevers, la curtea cărui a slujit restul vieții, exceptând unele perioade când a fost trimis în străinătate ca diplomat. În 1549, pe când avea 29 de ani, a fost trimis la Roma. Aici, Vigenere a luat contact cu problemele criptologice care l-au atras în mod deosebit. A citit lucrările lui Trithemius, Belaso, Cardano și Porta, precum și manuscrisul lucrării lui Alberti.

În timpul vieții sale a publicat vreo douăzeci de cărți, pe teme foarte ciudate, dar exceptând vestitul *Traicté des Chiffres* scris de des citat de traductori din acest domeniu, restul a căzut pradă uitării.

Acest „*Traicté*” este o lucrare curioasă. În cele peste 600 de pagini sunt cuprinse nu numai cunoștințele criptologice din vremea aceea, dar și un amestec ciudat de fapte și anecdote. Aici se găsește prima reprezentare europeană a ideogramelor japoneze. În digresiunile sale, Vigenere se ocupă de alchimie, magie, misterele universului, recipiente pentru prelucrarea aurului și face speculații filozofice de tipul „toate lucrurile din lume sînt un cifru”.

În ciuda acestor fantasmagorii, Traicte-ul, în ceea ce privește problemele criptologiei, merită toată crezarea. Vigenère a fost foarte scrupulos în ceea ce privește acest domeniu și toate informațiile pe care le dă sunt verificate cu grijă și redată cu acuratețe.

Printre numeroasele cifruri pe care le-a prezentat și comentat, Vigenère s-a oprit deosebit asupra cifrurilor polialfabetice. Fiecare din aceste cifruri se bazează pe tabloul lui Trithemius, deși Vigenère a așezat alfabetele mixte la capul orizontal și cel vertical al tabloului. A înregistrat și comentat o varietate largă de chei: cuvinte, expresii, versuri, data expediției, numele, funcția progresivă a tuturor alfabetelor etc. În cele din urmă, prezentă și procedeul său bazat pe autocheie. La fel ca și Cardano folosea textul clar drept cheie. Dar, spre deosebire de Cardano, a adus două perfecționări sistemului respectiv. În primul rând, el a asigurat sistemului o cheie primară, care este o singură literă cunoscută atât cifrului expeditor cât și cifrului destinatar. Această cheie primară ajută pe expeditor să poată începe descifrarea. Cu cheia respectivă, află prima literă din textul clar, care, la rândul ei, era cheia celei de a doua litere ș.a.m.d.

În al doilea rând, Vigenère, spre deosebire de Cardano, nu reîncepe cuvântul cheie la fiecare cuvânt din textul clar, ci folosește curent, în ordine, toate cuvintele și literele acestui text.

cheie — DA UNO MD ELETERNE

text clar — au nom de l'éternel

text cifrat — XI AHG UP TMLSHXT

În exemplul de mai sus, litera „D” constituie cheia primară. Procedeul acesta asigură o rezistență destul de mare,

fapt care a făcut ca în prezent să fie folosită și la unele tipuri de mașini de cifrat.

Vigenère a mai prezentat și un al doilea procedeu în care, după o cheie primară, autocheia constituie chiar criptograma:

cheie — DX HEE CO UMXGMABQ

text clar — au nom de l'éternel

text cifrat — XH EEC CU MXGANABQO

Acest procedeu are avantajul de a avea o cheie incoerentă, dar, în același timp, lasă cheia la dispoziția criptanalistului.

În ciuda expunerii foarte clare făcută de Vigenère asupra acestor procedee, ambele au fost complet uitate și au intrat în criptologia practică de-abia în secolul al XIX-lea.

Cifrul inspirat din Vigenère folosește azi doar alfabetele standard și o cheie formată dintr-un singur cuvânt care se repetă — un sistem mult mai susceptibil de a fi soluționat decât procedeul autocheii. Tabloul actual al sistemului Vigenère constă dintr-o tabula recta modernă — 26 de alfabet standard, așezate orizontal, fiecare fiind cu o literă mai înainte decât celălalt. Acestea sunt alfabetele cifru. Un alt alfabet normal este așezat pe verticală, în stînga tabloului, acesta fiind alfabetul cheie. Ambii corespondenți trebuie să cunoască cuvântul cheie. Cifrul repetă acest cuvânt deasupra literelor textului clar pînă cînd fiecare are un echivalent în cheie, după care caută litera textului clar în alfabetul de deasupra tabloului, iar litera din cuvântul cheie în alfabetul vertical. Litera aflată la intersecția alfabetului vertical al literei clare cu alfabetul orizontal al literei de cifrat constituie echivalentul folosit pentru cifrare. Pentru a se executa descifrarea, se începe cu litera din cheie, se găsește alfabetul de cifrat, cautînd litera din textul cifrat, după

În ciuda acestor fantasmagorii, Traicte-ul, în ceea ce privește problemele criptologiei, merită toată crezarea. Vigenère a fost foarte scrupulos în ceea ce privește acest domeniu și toate informațiile pe care le dă sînt verificate cu grijă și redată cu acuratețe.

Printre numeroasele cifruri pe care le-a prezentat și comentat Vigenère s-a oprit îndeosebi asupra cifrurilor polialfabetice. Fiecare din aceste cifruri se baza pe tabloul lui Trithemius, deși Vigenère a așezat alfabetele mixte la capul orizontal și cel vertical al tabloului. A înregistrat și comentat o varietate largă de chei: cuvinte, expresii, versuri, data expedierii mesajului, folosirea progresivă a tuturor alfabetelor etc. În cele din urmă, prezintă și procedeul său bazat pe autocheie. La fel ca și Cardano, el a ales a textul clar drept cheie. Dar, spre deosebire de Cardano, a adăugat două perfecționări sistemului respectiv. În primul rînd, el a asigurat sistemului o cheie primară, care, dintr-o singură literă cunoscută alături de cifrului expedierii, constituie cheia destinată. Această cheie primară ajută pe cititor să găsească începutul descifrării. Cu cheia respectivă, el află prima literă din textul clar, care, la rîndul ei, era cheia celei de a doua litere ș.a.m.d.

În al doilea rînd, Vigenère, spre deosebire de Cardano, nu reîncepe cuvîntul cheie la fiecare cuvînt din textul clar, ci folosește curent, în ordine, toate cuvintele și literele acestui text.

cheie — DA UNO MD ELETERNE
text clar — au nom de l'éternel
text cifrat — XI AHG UP TMLSHIXT

În exemplul de mai sus, litera „D” constituie cheia primară. Procedeul acesta asigură o rezistență destul de mare,

fapt care a făcut ca în prezent să fie folosit și la unele tipuri de mașini de cifrat.

Vigenère a mai prezentat și un al doilea procedeu în care, după o cheie primară, autocheia constituie chiar criptograma:

cheie — DX HEE CO UMXGMABQ
text clar — au nom de l'éternel
text cifrat — XH EEC CU MXGANABQO

Acest procedeu are avantajul de a avea o cheie incoerentă, dar, în același timp, lasă cheia la dispoziția criptanalistului.

În ciuda expunerii foarte clare făcută de Vigenère asupra acestor procedee, ambele au fost complet uitate și au intrat în criptologia practică de-abia în secolul al XIX-lea.

Cifrul inspirat din Vigenère folosește azi doar alfabetele standard și o cheie formată dintr-un singur cuvînt care se repetă — un sistem mult mai susceptibil de a fi soluționat decît procedeul autocheie. Tabloul actual al sistemului Vigenère constă dintr-o tabula recta modernă: 26 de alfabet standard, așezate orizontal, fiecare fiind cu o literă mai înainte decît celalalt. Acestea sînt alfabetele cifru. Un alt alfabet normal este așezat pe verticală, în stînga tabloului, acesta fiind alfabetul cheie. Ambele corespondențe trebuie să cunoască cuvîntul cheie. Cifrul repetă acest cuvînt deasupra literelor textului clar pînă cînd fiecare are un echivalent în cheie, după care caută litera textului clar în alfabetul de deasupra tabloului, iar litera din cuvîntul cheie în alfabetul vertical. Litera aflată la intersecția alfabetului vertical al literei clare cu alfabetul orizontal al literei de cifrat constituie echivalentul folosit pentru cifrare. Pentru a se executa descifrarea se începe cu litera din cheie se găsește alfabetul de cifrat, cautînd litera din textul cifrat, după

care, pe coloana alfabetului de deasupra se află litera din textul clar. De exemplu

cheie TYPE TYPE TYPE TYPE TYPE TYPE

text clar no is the time for all good

text cifrat GMLMLR WIMTMGBI YMGE EJUS...

În mod evident, acest sistem este mai vulnerabil decât originalul Vigenère, deși o legendă a circulat mult timp, susținând că el nu poate fi spart. Faptele aveau să dovedească contrariul.

CONTRIBUȚIA DILETANȚILOR

Telegraful a făcut din criptografie ceea ce este astăzi. În 1845 Francis O. J. Smith a publicat un cod intitulat „Vocabular de corespondență secretă adaptat pentru folosirea telegrafului magnetic”. În prefața acestei lucrări, autorul ei declara că „secretul corespondenței este de o importanță deosebită”. Această lucrare a stîrnit interesul unui mare număr de intelectuali, oameni de afaceri și politici pentru scrierile ascunse. Ei și-au adus din plin contribuția la îmbogățirea zestre de sisteme de cifrare a criptologiei.

Între timp, telegraful — autorul real al revoluției criptografice — a dus la apariția transmisiunilor din armată, iar o dată cu acestea a apărut și posibilitatea interceptării mesajelor, impunîndu-se cu necesitate o protecție a lor. Vechile nomenclatoare și noile coduri nu prezentau garanții în ce privește rezistența la criptanaliză și nu asigurau nici expeditivitatea cerută de mijloacele de comunicare.

Ofițerii de transmisiuni au părăsit codurile și nomenclatoarele și și-au îndreptat atenția spre cifruri, care puteau fi tipărite pe o foaie de hirtie și distribuite cu ușurință tuturor unităților interesate. Secretul putea fi asigurat de cheile variabile care se schimbau foarte repede. Cifrurile erau ideale pentru comunicațiile din zonele fronturilor și astfel a luat naștere, în perioada respectivă, ceea ce se numește cifrul militar.

La dispoziția militarilor se găsea, pe atunci, sistemul Vigenere modernizat. Vechile obiecte împotriva folosirii lui au dispărut o dată cu apariția telegrafului, iar reputația acestuia de a fi indestructibil i-a determinat pe militari să-l adopte fără rezerve.

Apoi, în 1863, un maior de infanterie din armata prusacă a descoperit soluția generală pentru cifrurile bazate pe substituția polialfabetică periodică. Dintr-o singură lovitură, vechea legendă a invincibilității lor s-a spulberat, iar ofițerii de transmisiuni, obligați să asigure secretul mesajelor pe care le transmiteau, au început să caute noi sisteme. Multe idei interesante s-au putut înscrive în criptografulor diletanți care propuneau diferite cifrări pentru mesaje particulare.

O mare parte din sistemele acestea de cifrare au devenit cunoscute și folosite cu succes și astăzi.

Unul din sistemele inventate înaintea apariției telegrafului depășea cu mult realizările epocii respective și era atât de mult în spiritul noilor invenții încât se impune să fie tratat împreună cu ele. Acest sistem este în același timp atât de modern ca și cel al lui Vigenere, de astăzi, după un secol și jumătate de progres tehnic rapid, continuă să fie folosit. Inventatorul său, Thomas Jefferson a fost un om politic și de cultură remarcabil. El a inventat „roata de cifrat” pe când era secretar de stat și voia să apere secretele S.U.A. față de Anglia și Franța, dar când bine să-l lăsa pe Jefferson să-și explice sistemul de cifrare:

„Luați un cilindru din lemn de vreo cinci centimetri diametru și 15 sau 20 cm lungime. Găuriți-l și introduceți înăuntrul unui ax. Împărțiți partea exterioară în douăzeci și șase de părți egale (pe care le va reprezenta alfabetul) și cu un vârf ascuțit, trageți linii paralele prin toate punctele de diviziune de la un capăt la altul al cilindrului. Trageți linii respective cu cerneală pentru a fi vizibile, apoi tăiați cilindrul în rotile foarte subțiri, de aproximativ jumătate de centimetru grosime. Numiți rotile pe părțile lor de la un capăt să le puteți aranja în ordine pe care o doriți. Pe partea exterioară a rotilei, între liniile trasate

cu cerneală, treceți toate literele alfabetului, nu în ordinea lor normală, ci la întâmplare, în așa fel încât să nu fie două rotile la fel. După ce ați terminat această operație, puneți-le pe axul de fier care are la cap o piuliță, pentru a putea stringe și imobiliza rotilele ori de câte ori doriți. Acum aparatul este gata pentru a fi folosit, dacă, bineînțeles, cei doi corespondenți au fiecare câte un aparat similar, cu rotilele așezate în mod identic.

Să presupunem că trebuie să cifram următoarea propoziție: „Your favor of the 22^d is received”.

Întorc prima rotă până apare litera y,

întorc a doua rotă până când în dreptul lui y, de pe prima rotă, apare o,

— întorc a treia rotă și-l așez pe u de pe a doua în dreptul lui o de pe a doua rotă,

— întorc a patra... până ce r este în dreptul lui u de pe a treia...

— întorc a cincea... până ce f este în dreptul lui r de pe a patra;

— întorc și a șasea... până ce a este în dreptul lui f de pe a cincea.

Fac această operație până când am toate cuvintele din propoziție aranjate într-un singur rând, apoi string rotilele cu șurubul. Veți observa că pe cilindru se găsesc alte 26 de șiruri, nu în serii regulate, ci amestecate, fără să aibă vreun înțeles.

Copiați oricare dintre ele și trimiteți-l corespondentului dumneavoastră. Când îl va primi, va aranja rotilele din care-l compus cilindrul, astfel încât să obțină și el șirul pe care l-ați trimis. După aceasta, fixează rotilele cu ajutorul șurubului, examinează celelalte 25 de șiruri rezultate și găsește unul în care scrie „Your favor of the 22^d is received”. Pe acesta îl reține, deoarece toate celelalte șiruri nu formează cuvinte inteligibile.

Când cilindrul de rotile este fixat și literele lor amestecate, apare o varietate imensă de cifruri pe care le puteți folosi simultan în corespondența cu diverse persoane care, deși au același aparat, nu vor putea afla secretul mesajelor transmise altcuiva, deoarece sînt criptate cu ajutorul altui cifru”.

acesta s-a stat imediat sub formă de pătrat. Ocupându-se în continuare de perfecționarea a acestui sistem, Wheatstone a folosit un alfabet de cifrat mai pe care l-a obținut prin transpoziție cu ajutorul unei chei. Procedul întrebuintat era cu totul nou și consta în următoarele: se scrie cuvantul cheie și dedesubt, în restul literelor alfabetului, după modelul de mai jos:

MAGNETIC
BDFHJKLO
PQRSUVWX
YZ

Retranscriind coloanele pe orizontală, a apărut următorul alfabet de cifrat: M B P Y A D Q Z G F R N H S E J U T K V I L W C O X. Ca și în cazul lui Vigenere, această posibilitate de a scrie alfabetul de cifrat a fost însă pierdută deoarece s-a recurs la forma cea mai imperfectă pe care o putea îmbrăca procedeul. Cheia a fost transcrisă direct într-un pătrat de 5x5 și nu în cele două rânduri de mai sus după modelul expus mai sus. Această formă a slăbit rezistența cifrului, dar a ușurat manevrarea lui, lată cum arată un astfel de cifru având drept cheie numele propriu PALMERSTON:

PALME
RSTON
BCDFG
HIKQU
VWXYZ

Pentru cifrat, textul e împărțit în grupuri de cîte două litere în litere duble cum ar fi în balcan, sunt despărțite într-o pereche în r, în a și în restul cuvintului respectiv va fi cifrat cu același cheie.

Literele din fiecare pereche pot intra în funcție de pătrat în următoarele raporturi: pot apărea pe același rând, în aceeași coloană sau nu și pe același rând, nu, pe aceeași coloană. Literele care cad în același rând sunt înlocuite cu următoarea literă din dreapta. Astfel, $em = LE$, $hi = IX$ și $os =$

NT . Fiecare rând este considerat ca fiind ciclic, așa că litera care urmează după ultima literă dintr-un rând este prima din rândul următor. Astfel, $le = MP$, $vi = HK$.

Literele care apar în aceeași coloană sînt înlocuite de literele aflate imediat sub ele.

Așadar, $oe = SJ$, $of = FQ$, $ui = AW$, $br = HB$. Dacă literele din textul respectiv de cifrat nu apar nici în rândul n în coloana pătratului, atunci sînt înlocuite cu literele din prima coloană și rîndul lor. Practic se procedează astfel: pentru a cifra secvența sq , cifrului trebuie să le caute în pătrat și, o dată identificate, urmărește rîndul literelor, pînă cînd acesta întâlnește coloana celei de-a doua litere și din secvența respectivă a lui Z.

M
RSTON
P
Q
Y

Litera aflată la intersecția șirului care îl conține pe s cu coloana în care se află q devine prima literă din textul cifrat. Apoi, cifra se continuă urmîndu-se de-a doua literă pînă cînd acesta intersectează coloana primei litere.

. A . . .
/S/ . . .
. C . . .
HIKQU
/W/ . . .

Litera aflată la intersecția rîndului care îl conține pe q cu coloana care îl conține pe s , aici t , devine cea de-a doua literă din textul cifrat. Descifrarea consta exact în același proces, ca și data $ow = SY$, atunci $sy = OW$. În primele două cazuri descrise, literele din textul cifrat se găsesc la stînga sau deasupra

literelor din textul cifrat. Folosind același pătrat, un text cifrat se reduce la următoarele :

MT TB BN ES WH TL MP TA LN NL NV
lo rd gr an vi lx le si et te rz

Z de la urmă este o literă fără valoare, pentru a completa grupa finală.

Avantajul unui astfel de cifru constă, în primul rând, în aceea că, fiind digrafic, ascunde caracteristicile literelor și reduce la zero eficiența metodelor obișnuite de analiză a frecvenței. De asemenea, înjumătățește numărul de elemente pentru analiza frecvenței. În al doilea rând, numărul de digrafe este cu mult mai mare decât numărul literelor simple și, în consecință, caracteristicile lingvistice se împart între mai multe elemente, ceea ce îngreuează mult individualizarea lor. Există numai 26 de litere față de 676 digrafe; cele mai frecvente litere din alfabetul englezesc e și t au o frecvență medie de 12, și respectiv 9 la sută; digrafele cele mai frecvente în engleză th și h au frecvență medie de numai 3,25 și 2,5 la sută. Cu alte cuvinte, nu numai că sînt mai multe unități dintre care trebuie făcută alegerea, dar acestea sînt mult mai puțin diferențiate între ele.

În Anglia, în 1857, se vindea un carton pe care se afla tipărit cu roșu și negru un pătrat conținînd alfabetul. Era un pătrat de carton alb, cu un pătrat de carton roșu în mijloc, pe care erau tipărite literele albe și negre. Pe marginea de sus a pătratului roșu erau scrise literele albe, iar pe marginea de jos a pătratului alb erau scrise literele negre. Acest pătrat era folosit pentru a indica poziția literelor în textul cifrat.

Într-un exemplu de cifru, se poate folosi un astfel de pătrat pentru a indica poziția literelor în textul cifrat. Dacă textul cifrat este "MT TB BN ES WH TL MP TA LN NL NV", atunci poziția literelor este indicată de următoarele litere: "lo rd gr an vi lx le si et te rz".

Pătratul alfabetic este în esență similar cu cel al lui Vigenere, cu excepția faptului că el reprezintă alfabetul normal pe toate cele patru laturi, iar pătratul lui Vigenere are doar două laturi cu litere.

gine se găsesc 17 litere și în fiecare cel al pătratului se află litera A.

Există și o altă variantă în care cifrarea începe nu cu litera din textul clar, ci cu cea din cheie. Această variantă s-a numit varianta Beaufort, dar poate fi numită și varianta Vigenere, deoarece funcționează în același mod ca și varianta Vigenere. Pentru a utiliza varianta Beaufort, se caută litera din cheie pe margine și litera din textul cifrat în rîndul prim al pătratului, iar la joncțiunea coloanei acestora cu rîndul literei din cheie se găsește litera din textul clar.

Tot în secolul trecut, americanul Phiny Earle Chase, la fel ca și Beaufort, a acordat pentru o foarte scurtă perioadă de timp atenție criptografiei, iar rezultatul a fost o invenție care a deschis noi drumuri în această știință. Astfel, printre articolele publicate de el în revista "The Atlantic Monthly", se află și un articol care descrie pentru prima dată un sistem de cifrat fracțional.

La baza acestui sistem se află cercul lui Polybius. Numelele de pe margine și de pe rîndul de deasupra indică rîndul și coloana în care se găsește o anumită literă. Pînă la Chase a apărut o serie întreagă de variante ale acestui cerc al lui Polybius, dar nimeni nu și-a dat seama că simbolurile pot fi folosite și pentru a indica poziția literelor în textul cifrat. Chase a despărțit cele două coordonate și le-a supus la diferite tratamente criptografice. El a început cu un cerc umplut cu zece coloane de litere grecești, ca cei pe care-i prezentăm mai jos :

	1	2	3	4	5	6	7	8	9	0
1	x	a	a	c	o	n	z	e	p	i
2	b	s	f	m	v	e	g	q	w	
3	d	k	s	v	h	r	a	t	i	r

Chase a scris vertical coordonatele, astfel încît cuvîntul "cat" Philip a devenit "1 3 3 1 3 1 3 1 3 1".

1 3 3 1 3 1
3 5 9 7 9 3

Un exemplu ne va ajuta să facem foarte uale cele spa-
mai sus. Luăm următoarea criptogramă :

ANYVG YSTYN RPLWH RDTKX
RNYPV QTGHP HZKFE YUMUS AYWVK ZYEZM
EZUDL JKTUL JLKQB JUQVUECKBN BKTHP
KESXM AZOEN SXGOL PGNLE EBMNT GCSSV
MRSEZ MXHLA KJESH TUPZU EDWKN NNRWA
GEEXS LKZUD LJKFI XHTKP IAZMX FACWC
TQIDU WBRRL TTKVN AJWVB REAWT NSEZM
OECSS VMRSI JMLEE BMNTG AYVIYGHPEM
YFARW AOAEL UPIUA YYMGE EMJQK SPCGU
GYBPJ BPZYPIJASN FSTUS STYVG YS

Repetițiile de cite trei litere sau mai multe au fost evi-
frecvente, deși in criptogramele mai scurte sint de un real
folos. Frecvența fiecărei litere este următoarea :

E S M Y T A K U L N P G J R Z V W B H C
22 18 16 16 15 14 14 14 13 13 13 13 11 11 10 9 8 8 7
X F D I Q O
7 6 5 5 5 4

Nu apar nici grupe de litere de frecvență înaltă, medie,
joasă sau mică. Avem de-a face cu o descriere lină, rezultat
al dispersării literelor individuale in citeva alfabet.

Nu apar nici grupe de litere de frecvență înaltă, medie,
joasă sau mică. Avem de-a face cu o descriere lină, rezultat
al dispersării literelor individuale in citeva alfabet.

O dată cu analiza se poate observa că în textul nostru
nu există grupuri de litere care să aibă o frecvență înaltă, medie
sau joasă. Acest lucru este datorat faptului că literele sunt
dispersate în mod egal în toate grupele de litere. Acest lucru
este datorat faptului că literele sunt dispersate în mod egal
în toate grupele de litere. Acest lucru este datorat faptului
că literele sunt dispersate în mod egal în toate grupele de
litere.

Repetiția	Prima	A doua	Intervalul	Factorii
YVGYS	3	283	280	$2 \times 2 \times 2 \times 5 \times 7$
STY	7	281	274	2×137
GHP	28	226	198	$2 \times 3 \times 3 \times 11$
ZUDLJK	52	148	96	$2 \times 2 \times 2 \times 2 \times 2 \times 3$
LEEBMMTG	99	213	114	$2 \times 2 \times 19$
SEZN	113	197	84	$2 \times 2 \times 3 \times 7$
ZMX	115	163	48	$2 \times 2 \times 2 \times 2 \times 3$
GEE	141	249	108	$2 \times 2 \times 3 \times 3 \times 3$

Cel mai frecvent factor este 2, care apare in fiecare caz,
dar deoarece 2 este factor in orice număr cu soș și deoarece
foarte rar se folosesc chei din două sau trei litere, criptanalistul
sau in considerație numai numerele de la 4 in sus. In tabelul
prezentat, 4 sau 2×2 este intilnit in cinci din cele opt intervale,
5 intr-un singur interval, 6 in șase intervale, 7 in două, 8 in
două, 9 in două, 12 in patru și celelalte (exceptind multipli
acestor numere) doar o singură dată.

La început, 6 pare să fie cea mai bună alegere luindu-se
criteriul frecvenței.

Criptanalistul retranscrie criptograma in zinduri de cite
șase litere, punind una sub alta toate literele despre care se
crede că au fost cifrate cu același alfabet. Apoi ia separat fie-
care coloană și încearcă să afle echivalentele din textul clar
pentru fiecare dintre ele. In cazul criptogramei noastre, in
prima coloană se găsesc 48 de litere, fiecare fiind cifrată cu
ajutorul primei litere din cheia de cifrare (adică este egal cu
numărul de litere din cheia) și acestea sint prima, a șaptea,
a treisprezecea etc. litera din cheia de cifrare.

ASLKVHUVZLJUKHMSGMSZKUWWSL
HZWUTJAZSJMVWUYJGJJSY.

Deși cifra arăta prea puțin, totuși frecvența literelor în această coloană reflecta o substituție monoalfabetică și nu o frecvență polialfabetică.

În cazul de față, situația frecvenței literelor se prezintă astfel:

2	0	0	1	0	2	4	0	5	3	3	3	0	0	0	0	5	1	4	2	4	0	2	4	
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T	U	V	W	X	Y	Z

Rezultatul este încurajator, chiar și numai pentru faptul că prima prezumție, conform căreia 6 ar fi numărul de litere din cuvântul cheie, este corectă.

Pentru ochiul experimentat, frecvența literelor în cazul nostru scoate în relief un profil normal al frecvenței în alfabetul englezesc.

Întrucât atât metoda de cifrare, cât și cea de decifrare, în cazul nostru, și cel folosit pentru cifrat sunt cunoscute, ambele fiind alfabetice, este posibil să se găsească o soluție. Într-adevăr, dacă se cunoaște metoda de cifrare, se poate găsi și metoda de decifrare. Frecvența literelor în textul cifrat este de 2, 0, 0, 1, 0, 2, 4, 0, 5, 3, 3, 3, 0, 0, 0, 0, 5, 1, 4, 2, 4, 0, 2, 4. Dacă se cunoaște metoda de cifrare, se poate găsi și metoda de decifrare. Frecvența literelor în textul cifrat este de 2, 0, 0, 1, 0, 2, 4, 0, 5, 3, 3, 3, 0, 0, 0, 0, 5, 1, 4, 2, 4, 0, 2, 4.

Clar: i j k l m n o p q r s t u v w x y z a b c d e
 Cifrat: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
 Clar: i j k l m n o p q r s t u v w x y z a b c d e
 Cifrat: X Y Z

Din tabel rezultă că i este substituit la A, j al lui B, k al lui C etc.

Această înșiruire poate fi utilizată astfel încât litera clară c să apară la m, p, a, având însă grijă ca echivalenții literă clară = literă cifrată să rămână aceiași.

Acuși echivalenți pentru cele 48 de litere din textul cifrat cu prima literă din cuvântul cheie, sunt următorii:

Cifrat: A S L K V H U W Z L J U K H M S G M S Z K U W
 Clar: i a t s d p c e h t r e s p u a o u a h s c e

Cifrat: W S L H Z W U T J A Z S J M V E W U Y J G J J S Y
 Clar: e a t p h e c b r i h a r u d m e c g r o r r a g

O astfel de grupare este acceptabilă și pare să ne ofere soluția.

Totuși, lucrul cel mai important pe care l-a aflat criptanalistul, după apariția în literatura alfabetică, este faptul că are de-a face cu un cifru de tip Vigenère. Această descoperire dă posibilitatea folosirii mai multor tehnici, bazate mai ales pe faptul că alfabetul este cunoscut. Metodele întrebuintate aici sunt valabile și pentru alte alfabete, dacă acestea sunt cunoscute criptanalistului și dau rezultate deosebite în cazul alfabetelor de tip Vigenère.

Una din aceste metode, care identifică literele în mod mecanic, folosește niște fișii de carton pe care alfabetul e tipărit de două ori. Literele de înaltă frecvență se tipăresc în diferite nuanțe de roșu, iar celelalte în negru. Criptanalistul așază aceste fișii una sub alta pentru a putea aranja în aceeași formape literele de aceeași culoare. Apoi se observă coloana care conține litere cu cea mai mare frecvență în textul respectiv.

Teoria probabilităților permite să se presupună că o coloană conținând litere de aceeași culoare este compusă în proporție de 42 la sută din literele de înaltă frecvență, în proporție de 61 %, dacă are 12 litere, de 74 %, dacă are 15 litere.

Dacă se ia și următoarea coloană, atunci probabilitatea crește la 74 %, 85 % și 90 %. În raport cu acest, metoda este aceea că 9 litere — o coloană — reprezintă o treime din alfabet, ceea ce înseamnă că majoritatea coloanelor vor fi colorate în roșu. Totuși, se poate și să se elimineze coloanele care conțin litere rare și să se elimineze cu albastru în tabelul de mai jos.

țiale. Ele sînt în număr de cinci, (γ, k, q, x, z) și împreună au o frecvență de aproximativ 2^{10} .

Căptanul nu va găsi decât va trece peste coloanele
care conțin tot sau o parte multe din lăturile evidențiate

Citru

to visit as possible

N	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	/	k	l	70
T	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	/	k	l	m	n	o	p	q	r	s
W	w	x	y	z	a	b	c	d	e	f	g	h	i	/	k	l	m	n	o	p	q	r	s	t	u	v
X	x	y	z	a	b	c	d	e	f	g	h	i	/	k	l	m	n	o	p	q	r	s	t	u	v	w
Y	y	z	a	b	c	d	e	f	g	h	i	/	k	l	m	n	o	p	q	r	s	t	u	v	w	x
Z	z	a	b	c	d	e	f	g	h	i	/	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y
A	a	b	c	d	e	f	g	h	i	/	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
B	b	c	d	e	f	g	h	i	/	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
C	c	d	e	f	g	h	i	/	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
D	d	e	f	g	h	i	/	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c

În urmare, numai coloana care începe cu literele f. l. o p.

te lito e a dan d' esse cato ho

12 .

124

THE HISTORY OF

I V T I T

10

References

、 p

V. 210. 2. 12.

51 1

LM¹¹, AY

1 4

W. H. Z. Y. F.

¶

LMELD

カ

INDEX

b6
b7C

J L K Q B J

1. 44

1 QV1 FC

()

K B N R C T

1 1

INDEX

FD

Criptanalistul e născut în acest fel, atât cît crede necesar, încercînd să deducă ori să ghicească unele litere sau cuvinte.

De exemplu, el știe că pentru a forma art. colul hotărât din limba engleză trebuie să fie precedat de t. În sistemul Vigenere, alfabetul literelor K este acela care ne dă rezultatul T — e. Se verifică rezultatul și se constată că este corect. T t corecte se dovedesc și celelalte e, l, n, t, u, v, m.

[illegible]

LIBRARY OF THE
LIEBMAN MUSEUM

frequent cu cheia GNALSIGN, iar următoarea repetiție ZUDIJK din cifrarea lui must be 's cu cheia NALSIG. Pe de altă parte repetiția ZUDIJK din cifrarea lui must be 's cu cheia GNALSIGN este în poziția 12 în cadrul grupului de 16 litere, în timp ce repetiția ZUDIJK din cifrarea lui must be 's este în poziția 10 în cadrul grupului de 16 litere. Repetiția ZUDIJK din cifrarea lui must be 's este în poziția 10 în cadrul grupului de 16 litere, în timp ce repetiția ZUDIJK din cifrarea lui must be 's este în poziția 12 în cadrul grupului de 16 litere. Repetiția ZUDIJK din cifrarea lui must be 's este în poziția 10 în cadrul grupului de 16 litere, în timp ce repetiția ZUDIJK din cifrarea lui must be 's este în poziția 12 în cadrul grupului de 16 litere.

Ce se întâmplă în cazul în care un copil are o
Criptanastafie este foarte rar. În acest caz, copilul
descoperire poate duce la o serie de complicații. În
oboseală, se recurge la diverse metode de tratament, pe baza carac-
terelor, a frecvenței și a altor factori. În unele cazuri, toate cele
form cu regulile folosite în tratamentul sunt de obicei

În limba română, rezistența unui inamic, aceston
r e trebuie să dia pe
care aceste schimbări ultimiza
Rezistența la descurare
mai des, iar mesaje e că

Se substituie prezumțiile în criptogramă și se construiește
textul din bucată cu bucată, descoperindu-se cheia
și alfabetul de cifrat. Pentru a avea șansa de succes în folo-
sirea acestor metode sunt necesare criptograme lungi, ca să fie
posibil să se găsească din elementele date, fiecare literă din cuvântul
chiar.

PROFESORUL, SOLDATUL ȘI OMUL DE GENIU

Profesorul de germană Auguste Kerckhoffs a intrat în
istoria criptologiei datorită contribuției sale la dezvoltarea
criptografiei militare. El a fost un om de știință, un inginer
telegrafic din Țările Basse. În 1883 a publicat o lucrare
cuprinzătoare în care a prezentat toate sistemele de cifrare
polialfabetice și alfabetele mixte existente pe vremea lui.

Însă ceea ce face din cartea lui Kerckhoffs o lucrare ca-
pitulă este faptul că el a pus în discuție condițiile care trebu-
rău să fie puse criptologiei de noile condiții, iar soluțiile propuse de el
sunt valabile, bine fundamentate și meritorii. Principala pro-
blemă constă în asigurarea securității comunicațiilor în condițiile
cerințelor noului sistem de comunicații creat prin apariția te-
legrafiei. Kerckhoffs a arătat că pentru a fi sigur, un sistem
după care să fie evaluat orice cifru ce urmează a fi folosit pe
timp de război.

În acest sens, el a făcut o diferență între sistemele de co-
municare militare din trecut și cele din prezent, și a arătat că un sistem de criptografie militară trebuie să în-
deplinească o serie de cerințe ca: simplitate, rezistență, expe-
ditivitate etc. Această subliniere a noulor cerințe constituie
prima contribuție a lui Kerckhoffs la dezvoltarea criptologiei.

A doua constă în reafirmarea principiului conform căruia
natura criptografiei trebuie să se bazeze pe principiul de
de cifrare.

Reacionând împotriva modelului simplu în care se analizează un sistem de cifrare, precum și împotriva încrederii nejustificate în aceste sisteme, Kerckhoffs a demonstrat că criptanaliza este singura metodă de decodificare a mesajelor și de aflarea adevărului despre diferite sisteme de criptare.

Din aceste două principii fundamentale în alegerea de mai jos, pentru fiecare sistem de criptare se cer unele specifice: 1) sistemul trebuie să fie indestructibil, dar și nu în teorie, ci în practică; 2) trebuie să fie ușor de înțeles și de folosit; 3) trebuie să fie ușor de memorat; 4) criptarea trebuie să fie ușor de realizat; 5) apărarea trebuie să fie ușor de realizat; 6) sistemul trebuie să fie ușor de realizat și de folosit. Este de presupus că un sistem de criptare trebuie să fie indestructibil, dar și nu în teorie, ci în practică.

Într-un sistem de criptare, mesajul este transformat într-un mesaj cifrat. Acest proces este realizat prin intermediul unei chei de criptare. Mesajul cifrat este apoi transmis prin canalul de comunicații. La recepție, mesajul cifrat este decodificat folosind aceeași cheie de criptare, astfel încât să se recupereze mesajul original. Acest proces este realizat prin intermediul unei chei de decodificare. Într-un sistem de criptare, mesajul este transformat într-un mesaj cifrat. Acest proces este realizat prin intermediul unei chei de criptare. Mesajul cifrat este apoi transmis prin canalul de comunicații. La recepție, mesajul cifrat este decodificat folosind aceeași cheie de criptare, astfel încât să se recupereze mesajul original. Acest proces este realizat prin intermediul unei chei de decodificare.

A răspuns Kerckhoffs, nu-i dădea să înțelegem că un sistem care necesită multă pară, fiind în mână mai multor indivizi, poate fi compromis oricând. Pară a devenit cu adevărat adevărul. Cea de-a doua concluzie formulată de Kerckhoffs a fost larg acceptată și reformulată astfel: în primul rând, cunoaște sistemul general de criptare, iar în al doilea rând, poți soluționa mesajul criptat folosind cheia de criptare. Cu alte cuvinte, după Kerckhoffs, trebuie să rezide numai în cheia.

Dacă Kerckhoffs ar fi putut prezenta o soluție mai bună, ar fi asigurat un loc în istoria criptologiei. El nu a făcut acest lucru. A pas la pas, el a demonstrat că un sistem de criptare trebuie să fie indestructibil, dar și nu în teorie, ci în practică.

Prima concluzie a lui Kerckhoffs este că un sistem de criptare trebuie să fie indestructibil, dar și nu în teorie, ci în practică. Cu alte cuvinte, trebuie să rezide numai în cheia. Mesajul cifrat este apoi transmis prin canalul de comunicații. La recepție, mesajul cifrat este decodificat folosind aceeași cheie de criptare, astfel încât să se recupereze mesajul original. Acest proces este realizat prin intermediul unei chei de decodificare.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	...
Mesajul 1	U	H	Y	B	R	J	I	M	B	C	F	A	M	M	T	
Mesajul 2	U	H	W	P	R	B	Q	L	K	I	B	L	W	R	E	
Mesajul 3	I	E	W	P	R	B	Q	L	K	I	B	L	W	R	E	
Mesajul 4	U	H	W	P	R	B	Q	L	K	I	B	L	W	R	E	
Mesajul 5	U	H	S	H	A	M	K	S	V	C	J	W	Z	V	X	...

Intrucât a fost folosită o singură cheie pentru cifrarea tuturor mesajelor, este clar că prima literă din cheie a ajutat la criptarea primei litere din fiecare mesaj. Deci, pe coloană apare unul din alfabetele de cifrat care nu constituie altceva

deci o substituție născută din cauza că, în practică, atacabilă după metoda frecvenței literelor. Același lucru este adevărat și cu privire la ceterile cifrări. Însă nu întotdeauna se poate procedea în acest mod, cînd avem în față un mesaj în care în fiecare mesaj cheie se mai deosebește. Iar exemplul este în cazul cheiei, PATRIE, pentru care mesajul în cifră este: P. A. T. R. I. E. În acest mesaj, prima literă va fi cifrăta cu cheia alfa. Pentru a afla cheia cifrării mesajului precedent sau al celui care urmează, trebuie să găsim cheia generată de litera e. Dacă în mesajul în cifră, după P. A. T. R. I. E. urmează cuvîntul: nu începe cu P. A. T. R. I. E. și după I. E. urmează mesajul anterior ultimului mesaj în cifră, după P. A. T. R. I. E. a fost A. Cu aceste cuvinte, se poate spune că este vorba de cifrarea unui singur mesaj foarte lung, dar care s-a făcut pe bucăți. În cazul acesta, criptanalistul trebuie să găsească cîteva repetiții pentru a putea face o suprapunere adecvată.

Cam acționează se poate observa în cazul un tabel cu
date maxie

Este evident că *N* și *E* sînt una lingă altă în fiecare alfabet de cifrat din acest tablou (considerînd alfabetele ca fiind cîmpuri asemănătoare *N* și *E* în alfabetul latin). Dacă un grup format din trei litere, *R* se află cu șase litere înaintea lui *B* etc. Astfel de relații pot fi stabilite între diferite litere din alfabetele respective, așa că, în cazul în care criptanalistul stabilește distanța dintre două litere din textul cifrat într-un alfabet și găsește una din aceste litere în alt alfabet, el poate plasa cea de-a doua literă la distanța cunoscută. Aceasta înseamnă că se stabilește un echivalent cifrat pe care nu l-a avut înainte și care poate fi înlocuit în toată criptograma pentru a adăuga câteva date care să ajute unei soluționări rapide.

clar	a b c d e f g h i j k l m n o p ...
alfabet de cifrat	K H
distanța	0 1 2 3 4 5 6 7 8 9

Apoi, să presupunem că, în alt alfabet, el a descoperit că litera de cifrat K îl reprezintă pe i din textul clar. Se numără 9 spații după K, astfel :

clar	a b c d e f g h i j k l m n o p q r s t u
alfabetul de cifrat nr. 2	K
distanța	0 1 2 3 4 5 6 7 8 9

și se oprește în întreg alfabetul identitatea $H = r$. Dacă se află, de exemplu, că litera e din textul clar este cifrată, în acest alfabet cu W, el va măsura distanța dintre K și W (patru litere) și va pune pe W ca pară spați înainte a lui K în primul alfabet de cifrat, găsind litera b din textul clar. Deoarece intervalele dintre litere rămân fixe pentru toate alfabetele de cifrat din acest tablou, identificarea corectă a citorva litere din alfabetele diferite duce la stabilirea celorlalte.

Kerckhoffs s-a oprit aici. Criptanalizistul au observat același lucru când au construit scheletul tablourilor pentru substituții de litere. Căci, deși alfabetul de cifrat este bazat pe alfabetul clar, el este totuși un alfabet de cifrat și nu poate fi decriptat decât prin intermediul alfabetului de cifrat. Uneori, asemenea înlocuiri în lanț duc la reconstituirea textului clar. Căci, dacă alfabetul de cifrat este bazat pe alfabetul clar, el este totuși un alfabet de cifrat și nu poate fi decriptat decât prin intermediul alfabetului de cifrat. Uneori, asemenea înlocuiri în lanț duc la reconstituirea textului clar. Căci, dacă alfabetul de cifrat este bazat pe alfabetul clar, el este totuși un alfabet de cifrat și nu poate fi decriptat decât prin intermediul alfabetului de cifrat.

Kerckhoffs și-a încununat opera prin popularizarea alune-
cării criptografice. El a publicat o lucrare intitulată „Système de cryptographie” în care el prezintă o serie de metode de cifrare și de decriptare. El a publicat o lucrare intitulată „Système de cryptographie” în care el prezintă o serie de metode de cifrare și de decriptare. El a publicat o lucrare intitulată „Système de cryptographie” în care el prezintă o serie de metode de cifrare și de decriptare.

Altfel, el pe stator reprezintă alfabetul textului clar iar alfabetul de pe alunecător alfabetul de cifrat.

Dacă ambele alfabetele sunt în ordinea normală, acest aparat dă naștere unei versiuni precitate a tabloului lui Vigenere, deoarece orice alfabet din tabloul respectiv poate fi reproducut, dându-i-se cheia pe alfabetul alunecător și așezându-l sub litera A a alfabetului de stator.

Cu ajutorul acestui dispozitiv, dacă litera din alfabetul de cifrat este în ordinea normală, se obține alfabetul de cifrat Kerckhoffs. Dacă litera din alfabetul de cifrat este în ordinea normală, se obține alfabetul de cifrat Kerckhoffs. Dacă litera din alfabetul de cifrat este în ordinea normală, se obține alfabetul de cifrat Kerckhoffs.

Aceasta este contribuția lui Kerckhoffs la dezvoltarea criptologiei și a criptoanalizei. El a publicat o lucrare intitulată „Système de cryptographie” în care el prezintă o serie de metode de cifrare și de decriptare.

Cartea lui Kerckhoffs a situat Franța în fruntea țărilor cu cea mai dezvoltată criptografie și, totodată, a dat un imbold neașteptat activităților din acest domeniu. O serie de amatori și profesioniști au căutat și descoperit noi sisteme de cifrare, dar majoritatea lor erau lipsite de originalitate, mulți dintre ei condensind și mai mult opera lui Kerckhoffs.

Un ofițer de infanterie și asistent al unui prefect de poliție, marchizul Gaëtan de Viaris, a început să se intereseze de criptografie și a inventat unele dintre primele mașini de cifrat care asigură și tipărirea, după cifrare, a criptogramei. Mecanismul mașinii era foarte simplu, singura operație pe care trebuia să o facă criptograful fiind aceea de a apăsa pe un buton care imprima litera de cifrat pe o fișă de hirtie. De asemenea, el a publicat pentru prima oară ceea ce s-au numit „ecuații criptografice”.

În articolele apărute în publicația științifică Le Gémme Civil, numerele din 12 și 19 mai, de Viaris propunea ca litera greacă χ (chi) să înlocuiască orice literă din textul cifrat, iar litera γ (gamma) orice literă din textul clar. El a demonstrat că formula $c + \gamma = \chi$ dă o cifrare de tipul Vigenere, al cărei alfabet este alfabetul de cifrat. El a publicat o lucrare intitulată „Système de cryptographie” în care el prezintă o serie de metode de cifrare și de decriptare.

alfabetului sunt numerotate de la 0 la 25, după modelul de mai jos :

a b c d e f g h i j k l m n o p q r s t u v w x y z
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

tabloul Vigenere poate fi dat în mai multe variante, adunându-se valoarea pentru litera clară și cea din cheie și apoi transformând suma în litera din alfabetul de răspundere. De exemplu, dacă litera clară este a și litera din cheie d, cu ajutorul tabelului Găsim litera j. Dacă litera clară este e și litera din cheie d, găsim litera i. Un alt cifru va avea, desigur, o altă formulă. Pentru cele trei mari sisteme polialfabetice moderne (cu literele C = litera clară, K = litera din cheie, C = litera cifru) :

$C + K = P$	$C - K = P$	$K - C = P$
$C + P = K$	$C - P = K$	$K - C = P$
$K + P = C$	$K - P = C$	$C - K = P$

Simetria acestor formule arată clar, aproape grafic, că

Matematica aplicată criptologiei a fost cea mai

... în 1818, la Viena, în timpul congresului de matematică...

Etienne Bazeries este cel mai mare specialist al criptologiei. Contribuția lui este în domeniul criptanalizei. El a descoperit mai multe sisteme de criptare și a dezvoltat metode de descifrare. Bazeries a lucrat pentru serviciul de securitate francez și a fost unul dintre cei mai buni criptanalizatori ai secolului al XIX-lea. El a scris multe cărți și articole despre criptologie și a fost unul dintre cei mai cunoscuți specialiști în domeniu.

stocare prea mult creierii".

... a fost un mare specialist în domeniul criptologiei. El a descoperit mai multe sisteme de criptare și a dezvoltat metode de descifrare. Bazeries a lucrat pentru serviciul de securitate francez și a fost unul dintre cei mai buni criptanalizatori ai secolului al XIX-lea.

cu 25 de litere pe circumferințele lor, în loc de 36 de discuri, și care conțineau întreg alfabetul.

Nici acest aparat n-a fost adoptat de Ministerul de Război, iar marchizul de Vianis s-a ambiționat să soluționeze trei mesaje trimise lui de către Bazeries și astfel a dat un suport deciziei luate de armată.

Metoda de soluționare cere ca criptanalistul să fie în posesia aparatului. Această presupunere era în concordanță cu principiul lui Kerckhoffs, conform căruia nici un sistem de cifrare militar nu trebuie să presupună ca aparatul folosit în cifrare să fie secret.

Bazeries a acceptat principiul și a ținut secretă doar cheia — ordinea în care discurile erau plasate pe ax — fiind sigur de imposibilitatea rezolvării mesajului. În metoda folosită de

prin a întoarce discurile în așa fel încît numai litera a se afîa pe rîndul „clar”. Fiecare rînd succesiv — numit generatrix — cuprinde toate echivalentele textului cifrat care pot exista pentru a pe respectivul generatrix. Mai mult decît atît, aranjamentul echivalenților pe fiecare generatrix diferă de celelalte. De exemplu, primul din generatrix sub a în aparatul lui Bazeries erau :

nr. discului	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
text clar	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a
generatrix 1	B	E	E	Z	Z	L	V	R	F	N	I	U	T	J	I	B	B	C	C	
generatrix 2	C	I	B	Y	X	O	D	Y	N	D	C	X	I	B	M	C	C	H	F	

Pentru a construi alfabetul ușor de reținut, Bazeries folosea chei de tipul : „Doamne apără Franța”, „Onoare și patrie” sau „Ferți-vă de curent”, „Instruiți tineretul” ori expresii ca : „Împac și pace pe pământ și în cer”. Alte alfabetice ar produce altele modele.

Acești doi generatrix folosesc diferite litere pentru a-l substitui pe a.

Criptanalistul poate să prezume că un cuvînt sau o parte din cuvînt, cum ar fi ation din criptogramă, a fost cifrat în întregime pe unul din generatrixurile aflate înaintea lui. Atunci el va încerca să substituiască pe a pentru a, t, i, o și n și le afîa în coloane una lîngă alta. Aceste coloane le suprapune pe criptogramă creînd un grup de cinci litere în care prima literă aparține pentru a, t, i, o și n, a doua pentru substituițele lui t și a a mai departe. Orice grup de acest fel, în mod evident, poate constitui un posibil echivalent pentru ation.

Să presupunem că criptanalistul a găsit un asemenea grup. Dacă substituiția pentru a în acel grup este t, discul folosit trebuie să fi fost numărul 8. Este singurul disc care substituie

cu t pe primul generatrix. Dacă substituiția era c, discul folosit putea fi 4, 5 sau 6. Alegerea pentru celelalte litere este, de asemenea, limitată. Criptanalistul asamblează discurile bazîndu-se pe aceste alegeri și, de aceea mesajul a fost cifrat cu douăzeci de litere o dată, încearcă descifrîr, la intervale de cîte cîte a găsit permutarea exactă a cîtorva discuri și, poate prin aranjarea, să mărească aceste însușiri într-un arhipelag și, în cele din urmă, să le unească într-un continent de text clar. Dacă nu apare nici un fel de text clar, criptanalistul trebuie să continue căutarea pe discurile rămase până apare o soluție. În cazul în care nu apare o soluție de probabilitate nu poate să treacă de pe prima parte a mesajului la a doua și a treia parte.

Întregul proces — ziceau la Vaux — este foarte mult timp și a fi explicat decît a fi făcut.

La cînda acestor exotice criptanaliste, la Vaux nu a avut încă idee că de Vaux și de Bazeries s-a găsit o soluție valabilă pentru cilindrii lui.

Respingerea cilindrilor nu l-a liniștit pe Bazeries, căruia i-a venit în minte să încerce să descifreze mesajele prin metoda de descifrare a discurilor. El a găsit o soluție valabilă pentru cilindrii lui.

Cheia era formată din două litere transformate într-un număr după regula $A = 1$, $B = 2$ și așa mai departe. Acest număr scris în cuvinte forma alfabetul de cifrat. Folosind alfabetul de cifrat SF devenea ONE HUNDRED FIFTY-SIX, dînd ca alfabet cheia ONE HUNDRED FIFTY-SIX. După ce textul clar era substituit cu alfabetul de cifrat, criptanalistul trebuia să găsească cîte trei litere în care se inversa ordinea. Se puteau, de asemenea, interpola vocale și nule pentru a întări sistemul, iar cheia

Toate aceste invenții în domeniul criptografiei se făceau pentru armată. Întreaga Europă care se pregătea de război era cuprinsă de febra criptologică. Ea voia să fie bine pusă la punct în această privință.

Războiul avea să dovedească justetea celor care și-au asigurat din timp un arsenal criptologic. Acesta i-a ajutat să dobândească multe victorii și să contracareze multe acțiuni inamice.

„CAMERA 40”

În ziua de 5 august 1914, prima zi a războiului care avea să se desfășoare la lătar după toate șansele, un torpedier german a lansat un torpedou în apropierea insulei de Funder, în estul mării Nord. Torpedoul a fost aruncat pe aer și a explodat în aer. În același timp au fost ridicate pe bord cablurile transatlantice care făceau legătura dintre Germania și America. După explozie, torpedoul a căzut și cablurile au căzut înapoi în mare, complet nefolositoare.

Din acel moment, Germania a fost nevoită să comunice cu străinătatea prin radio sau prin linii telefonice controlate de inamic. În felul acesta, ea dădea dușmanilor săi posibilitatea de a-i cunoaște cele mai secrete planuri și intenții, bineînțeles, dacă aceștia erau în stare să înlăture păienjenitul de cifruri și coduri care le ascundeau. Era o situație pentru care englezii nu erau pregătiți, dar n-au vrut să lase să le scape ocazia de a obține informații.

În acest sens, s-au luat măsuri de înființare a unui birou special care se ocupa cu decriptarea mesajelor interceptate de la inamic și în fruntea căruia a fost pus sir Alfred Ewing. Activitatea în acest birou a demarat destul de greu, englezii, la vremea aceea, fiind destul de ageamii în ce privește criptologia. În septembrie 1914, primul mesaj interceptat a fost decriptat în septembrie 1914.

a fost distrus pe când se afla în Marea Baltică. Cîteva ore mai tîrziu, rușii au pescuit din apele mării cadavrul unui subofiter german. Asupra acei tîm s-au găsit cifrul și tabelul de semne și semnale ale marinei de război germane. Rușii, considerînd că aceste documente prezentau interes pentru Anglia, pe atunci cea mai mare putere maritimă, au cerut ca o navă britanică să meargă la Petrograd ca să ia în primire prețioasa pradă de război. Cu toate că aveau cîrmă enelezilor le-a mai trebuit o perioadă de timp pentru să rezească să decodifice primele mesaje interceptate. Prin pricina faptului că constituia supracifrarea manuală textului, soluția destăruării unei asemenea supracifrări nu era prea diferită de cea necesară cînd ai cifru. Căci în textul de la amiralul german din cadrul textului cifrat sau decodificat se pot înscena disordine. Uneori anumite cifre din codificate se repetă după o anumită structură. În cazul codului german, consoanele alternau cu vocalele în grupe de cîte patru litere. Cînd se cunosc aceste lucruri, criptanalistul le remarcă imediat și le folosește pentru a soluționa supracifrarea.

Trei săptămîni le-au trebuit englezilor pînă au reușit să descodifice frînturi din mesajele interceptate de la nemți.

Între timp, Ewing a reușit să încadreze un număr mare de criptologi, iar acest serviciu a primit denumirea sub care avea să fie cunoscut de toată lumea: „Camera 40”.

În urma descifrării ordinului transmis unei flote din marina de război germană de a bombarda cîteva porturi britanice, Amiralitatea britanică a elaborat un plan prin care cîteva din cele mai puternice nave de război engleze au fost dirijate în zona prin care urma ca respectiva flotă să se reîntoarcă în Germania. Succesul a fost deplin. Timp de un an de zile, germanii n-au mai putut părăsi porturile din Marea Nordului, deoarece majoritatea navelor fuseseră avariate sau distruse, iar echipajele suferiseră pierderi grele.

Între timp, în marina germană din Balchica de supracifrare, de decodificare și de criptare s-a acumulat o cîtăreare experiență în învățarea războiului, le-a fost necesară doar o noapte pentru a înțelegi mesajele și ordinele transmise de nemți prin radio.

(1) caracteristică a perioadei, respectiv o constatarea faptului că nemții dădeau mare atenție războiului submarin. Cu toate acestea, în ciuda multelor măsuri de securitate pe care le lua, nu de puține ori submariniele lor erau interceptate.

În cele din urmă au început să se facă dețin codul și atunci au început să-l schimbe. Așa se face că în luna august 1916, pe întreaga flotă germană a fost schimbat codul. Dar la arădă „Camera 40” era atât de versatilă în decipțan încît Amiralitatea britanică nu a simțit lipsa informațiilor provenite din sursa sursă. Curînd după aceea, pentru a verifica justetea informațiilor găsite de criptologi, „Camera 40”, a fost recapturată de pe nava germană „Zepelin L-22” noul cod german, care a fost trimis la Amiralitatea britanică. Criptanalistii au dat o idee clară și valoarea informațiilor interceptate a ajutat să facă față condițiile de operații în Marea Nordului, din ce în ce mai pline de mesaje interceptate.

Pe măsură ce numărul de mesaje interceptate sporea, creștea și personalul „Camerei 40”. Acesta a devenit adevăratul centru al activității de criptologie. În timpul războiului, majoritatea celor care au lucrat în „Camera 40” au devenit profesori universitari, mulți în științele matematice, alții în literatură, română sau franceză. În acest sens, este interesant să se noteze că pînă și dactilografele, pentru a putea lucra la acest serviciu, trebuiau să cunoască cel puțin două limbi străine. Pe baza informațiilor primite de la „Camera 40”, flota germană a reușit să distruză majoritatea navelor de război germane. „Camera 40” a funcționat pe tot timpul primului război mondial și unul din cele mai mari succese l-a înregistrat în anul 1917. Acest succes merită să fie relatat, mai ales că el ilustrează rolul criptologiei în desfășurarea evenimentelor istorice.

În dimineața zilei de 17 ianuarie 1917, reverendul William Miller, care lucra în cadrul „Camerei 40”, a prezentat primul lord al amiralității un criptogramă pe care el o considera foarte importantă.

Criptograma era destul de lungă și conținea informații foarte importante. Era destul de o mie de cuvinte. În data la Berlin pe

ce mai rapid. La 28 ianuarie, de Grey i-a adus lui Hall un proiect al lui Bernstoff, ambasadorul german în S.U.A., împotriva planului lui Zimmermann de a declara un război submarin total. Bernstoff se pronunța cu hotărâre împotriva acestui plan, dăruindu-i, deosebi seama că planul lui în aplicare ar fi însemnat împotriva eficientelor pe care el le depunea în vederea unei destinderi între S.U.A. și Germania, fapt care ar fi împiedicat intrarea Statelor Unite în război de partea Antantei.

La 3 februarie, Wilson, preşedintele S.U.A., a anunţat Congresului că va război cu Germania dacă aceasta va declanşa un război submarin total, dar preciza că va face acest lucru doar în cazul în care „faptele vor arăta că nemţii scufundă în mod deliberat vasele ţărilor neutre ce navighează în apele internaţionale”.

În timp ce pe 5 februarie, la 14.00, de Grey a mai reușit, cunoscând din alte surse conținutul convorbirii ce a avut loc între Wilson și Bernstoff, să soluționeze și alte grupe din codul respectiv. Facind substituțiile care se impuneau, la 5 februarie de Grey era în măsură să descifreze aproape în întregime telegrama lui Zimmermann.

Hall apreciasse încă din prima zi că această telegramă reprezenta o valoare de proporții deosebite. Demascarea publică sau pe canale diplomatice a intențiilor Germaniei, care aduceau o atingere directă intereselor S.U.A., în condițiile date, obligau guvernul american să declare război Imperiului German. În acest sens, telegrama era o dovadă evidentă care trebuia prezentată fără întârziere americanilor, dar, pentru moment, motive mai puternice îi opreau pe englezi s-o facă. Primul motiv era acela că existența „Camerei 40” și posibilitățile de cîmpionat ale serviciilor de securitate erau cunoscute unul de altul și erau importante pentru ambele țări. Al doilea. Cum se putea ști că, fără această telegramă, s-ar fi putut afla că englezii erau în posesia unei informații atât de importante? Se putea spune că telegrama fusese interceptată, dar aceasta presupunea ca deștep să bătă la scapă adevărul și să schimbe codul. În al doilea rînd, dacă englezii arătau telegrama și ar fi spus că au interceptat-o,

[illegible]

1. In-ataama, t...
 2. ...
 3. ...
 4. ...
 5. ...
 6. ...

În consecință, a conceput un plan care, dintr-o singură lovitură, înlătura trei din motivele care îi împiedicau pe englezi să se folosească de telegramă.

Intrucit telegrama fusese trimisa mai intai la Washington, s-a putut recodifica textul originalului, aducand din nou la forma pe care a avut-o inainte de a fi trimisa la Berlin. In Mexic, s-a presupus ca ea suferise unele mici modificari de forma, cum ar fi: schimbarea datei expedierii ei si preambulul. Deci, daca s-a putut sa faca tot ce trebuia, s-a putut sa se faca tot ce trebuia. Si astfel, pe 17 februarie, Mexicul a primit din nou telegrama lui Zimmermann. In acelasi timp, s-a putut sa se faca tot ce trebuia. Si astfel, pe 17 februarie, Mexicul a primit din nou telegrama lui Zimmermann. In acelasi timp, s-a putut sa se faca tot ce trebuia. Si astfel, pe 17 februarie, Mexicul a primit din nou telegrama lui Zimmermann.

Într-un cod care n-ar fi fost de mirare, să fi fost soluționat
cândva de englezi.

Începând cu 5 februarie, Hall a ordonat să se caute cu in-
sistență o copie a telegramelor a căror a sursă ea în Mexic. Un
agent englez cunoscut doar după inițiala „T.” a obținut de la
oficiul telegrafic din Mexic o copie a mesajului lui Bernstoff
către Eckardt.

Toate prezumțiile făcute s-au confirmat. Eckardt nu avea
codul 0075, așa că telegrama fusese recodificată, iar codul fo-
losit nu era altul decât codul 13040, un cod mai vechi și mai
ușor de soluționat decât 0075. Codul 13040, distribuit misiunilor
diplomatice germane din țările latino-americane, conținea
250 000 de elemente clare și un număr destul de mare de homo-
fone — numai în telegrama lui Bernstoff se foloseau șase gru-
puri de cifre diferite pentru ze, iar numele proprii aveau peste
75 000 de echivalenți. Dar codul 13040 era o combinație între
un sistem de cod simplu și unul dublu. În partea de cod, grupu-
rile de echivalenți aranjate în ordine numerică crescândă erau
opuse elementelor clare aflate în ordine alfabetică. Spre ilus-
trare, dăm câteva secțiuni din cod :

13605 Februar	4377 geheim
13732 fest	4458 Gemeinsame
13850 finanzielle	5144 wenigen
13918 folgender	5161 werden
17142 Frieden	5275 Anregung
17149 Friedensschluss	5376 Anwendung
17166 fuhrung	5454 ar
17214 Ganz geheim	5569 auf
17388 Gebert	5905 Krieg

Soluționarea unui astfel de cod hibrid este mai ușoară
decât în cazul unui cod complex și mai grea decât cea a unui
cod simplu. Ordinea numerică este ușor de găsit din grupurile respec-
tive, întrucât multe pe grupuri sunt, dar ghicirea nu mai este atât
de sigură în cazul codului simplu. De exemplu, criptanalistul

nu poate spune că cifra care reprezintă cuvântul Krieg este un
număr mai mare decât cel care-l reprezintă pe Februar. Dar,
dacă a aflat că Februar = 13605 și finanzielle este 13950,
atunci pentru el e clar că fost este prezentat de un număr
mai mare între cele două. Identificarea în acest caz, sunt mai ra-
zătoare mai sigure.

Într-o altă această slăbiciune este faptul că în timpul
criptanalizei, Când Hall a descoperit că na era un mare
număr de mesaje, codul 13040 a fost folosit aproape în întregime.
În acest cod procedurile erau foarte simple și ușor de înțeles.
În partea din mesajul lui Bernstoff, de exemplu, erau
cuvinte cunoscute nume proprii, care erau folosite pentru prima
oară în alfabetul alfabetic, dar erau prezentate în ordine
numerică. În plus, sunt lucruri care erau date ca se știa
de la început pentru descurcarea mesajului. De exemplu, Bernstoff
a fost bine cunoscut în timpul războiului, întrucât în acest
cod a fost folosit codul 13040.

Tot cu această ocazie s-au adeverit și presupunerile lui
Hall. Bernstoff înlocuise preambulul Ministerului de Externe
german cu unul personal.

De asemenea, mesajul purta data de 19 ianuarie, în loc
de 16 cit era în original, iar numărul de serie dat de Berlin era
înlocuit cu unul propriu.

În februarie, Hall era gata de acțiune. Ideea lui genială
avea să dea roade. Această acțiune de conspirare a sursei de
unde provenise informația este una dintre cele mai subtile.
Acum era posibil ca telegrama să fie dată americanilor cu
faptul că ne riscăm de a fi descoperiți de informații
ale serviciului secret. Deși ștersese urmele, Hall nu s-a grăbit
să transmită informația americanilor, ci a stat să m-
aștepte să vadă cum evolua situația. Așa că cu atât
mai mult cu cât prevederile erau mai bune, pe lângă faptul
că Hall nu punea să fie descoperit de americani. În acest
moment, care să-l dovedea că era în posesia informației în mod pre-
cizat, navele de transport erau în cale din armă, cum
era și străduindu-se din război să se facă asemenea
faptelor înarmatori, iar în acest se pe front se înălțau

pe vocueta și de a înălța acțiunile întreprinse de germani nu sînt altceva decît operațiuni de război, împotriva poporului Statelor Unite.

Așa se face că soluția găsită de „Camera 404” a telegramelor trimisă de inamic a permis grăbirea intrării în război și, în final, cîștigarea lui.

RAZBOIUL INTERCEPTĂRIILOR

Când a izbucnit războiul, în 1914, de vedea că cîștigul era al Franței, care era pregătită. În acel moment, secția criptologică a Ministerului de Război era în plină dezvoltare, iar stațiile de interceptare se înmulțiseră. „Franczii — a declarat Cartier, șeful secției criptologice — au interceptat în timpul războiului mai multe mesaje de mare interes, unele mesaje care ar forma o bibliotecă de 1 000 de romane de grosime medie”.

Ei au reușit să spargă cifrul german UBCHI, bazat pe o transpoziție pe două coloane și o cheie care, înainte de cifrare, era transformată într-o secvență numerică. Această operație se făcea dînd valori numerice literelor din cheie, luate în ordine alfabetică. În cazul în care unele litere se repetau, fiecare dintre ele primea o altă valoare numerică ce creștea de la stînga la dreapta. Dacă luăm ca exemplu cheia DIE WACHT AM RHEIN, obținem: D 3, I 2, E 5, W 6, A 4, C 1, H 7, T 8, A 4, M 9, R 10, H 7, E 5, I 2, N 11. Dacă luăm ca exemplu mesajul: DIE WACHT AM RHEIN, obținem: 3 2 5 6 4 1 7 8 4 9 10 7 5 2 11. Dacă luăm ca exemplu cheia DIE WACHT AM RHEIN, obținem: D 3, I 2, E 5, W 6, A 4, C 1, H 7, T 8, A 4, M 9, R 10, H 7, E 5, I 2, N 11. Dacă luăm ca exemplu mesajul: DIE WACHT AM RHEIN, obținem: 3 2 5 6 4 1 7 8 4 9 10 7 5 2 11.

DIE WACHT AM RHEIN

495 1513714 211 13861012

Cifrarea unui text clar, să spunem: Tenth division X at Montigny sector, se face în șase etape separate. you ! implică șase etape separate.

În limba română: „Divizia a zecea X atacă sectorul Montigny în zorii zilei X. Va fi precedată de un baraj de gaze”.

1. Cifrorul scrie textul clar orizontal sub formă de tabel
sub secvența de numere din cheie :

[illegible]

2. Transcrie literele din coloane în ordinea naturală a
 1. 2. 3. 4. 5. 6. 7. 8. 9. 10. 11. 12. 13. 14. 15. 16. 17. 18. 19. 20.
 HECAY, ITYG, LMIU
 așa mai departe.

3. Le transcrie orizontal in alt tabel sub aceeași cheie.

4. În tabelul obținut mai adăugăm exact același număr de
 1. 2. 3. 4. 5. 6. 7. 8. 9. 10. 11. 12. 13. 14. 15. 16. 17. 18. 19. 20. 21. 22. 23. 24. 25. 26. 27. 28. 29. 30. 31. 32. 33. 34. 35. 36. 37. 38. 39. 40. 41. 42. 43. 44. 45. 46. 47. 48. 49. 50. 51. 52. 53. 54. 55. 56. 57. 58. 59. 60. 61. 62. 63. 64. 65. 66. 67. 68. 69. 70. 71. 72. 73. 74. 75. 76. 77. 78. 79. 80. 81. 82. 83. 84. 85. 86. 87. 88. 89. 90. 91. 92. 93. 94. 95. 96. 97. 98. 99. 100. 101. 102. 103. 104. 105. 106. 107. 108. 109. 110. 111. 112. 113. 114. 115. 116. 117. 118. 119. 120. 121. 122. 123. 124. 125. 126. 127. 128. 129. 130. 131. 132. 133. 134. 135. 136. 137. 138. 139. 140. 141. 142. 143. 144. 145. 146. 147. 148. 149. 150. 151. 152. 153. 154. 155. 156. 157. 158. 159. 160. 161. 162. 163. 164. 165. 166. 167. 168. 169. 170. 171. 172. 173. 174. 175. 176. 177. 178. 179. 180. 181. 182. 183. 184. 185. 186. 187. 188. 189. 190. 191. 192. 193. 194. 195. 196. 197. 198. 199. 200. 201. 202. 203. 204. 205. 206. 207. 208. 209. 210. 211. 212. 213. 214. 215. 216. 217. 218. 219. 220. 221. 222. 223. 224. 225. 226. 227. 228. 229. 230. 231. 232. 233. 234. 235. 236. 237. 238. 239. 240. 241. 242. 243. 244. 245. 246. 247. 248. 249. 250. 251. 252. 253. 254. 255. 256. 257. 258. 259. 260. 261. 262. 263. 264. 265. 266. 267. 268. 269. 270. 271. 272. 273. 274. 275. 276. 277. 278. 279. 280. 281. 282. 283. 284. 285. 286. 287. 288. 289. 290. 291. 292. 293. 294. 295. 296. 297. 298. 299. 300. 301. 302. 303. 304. 305. 306. 307. 308. 309. 310. 311. 312. 313. 314. 315. 316. 317. 318. 319. 320. 321. 322. 323. 324. 325. 326. 327. 328. 329. 330. 331. 332. 333. 334. 335. 336. 337. 338. 339. 340. 341. 342. 343. 344. 345. 346. 347. 348. 349. 350. 351. 352. 353. 354. 355. 356. 357. 358. 359. 360. 361. 362. 363. 364. 365. 366. 367. 368. 369. 370. 371. 372. 373. 374. 375. 376. 377. 378. 379. 380. 381. 382. 383. 384. 385. 386. 387. 388. 389. 390. 391. 392. 393. 394. 395. 396. 397. 398. 399. 400. 401. 402. 403. 404. 405. 406. 407. 408. 409. 410. 411. 412. 413. 414. 415. 416. 417. 418. 419. 420. 421. 422. 423. 424. 425. 426. 427. 428. 429. 430. 431. 432. 433. 434. 435. 436. 437. 438. 439. 440. 441. 442. 443. 444. 445. 446. 447. 448. 449. 450. 451. 452. 453. 454. 455. 456. 457. 458. 459. 460. 461. 462. 463. 464. 465. 466. 467. 468. 469. 470. 471. 472. 473. 474. 475. 476. 477. 478. 479. 480. 481. 482. 483. 484. 485. 486. 487. 488. 489. 490. 491. 492. 493. 494. 495. 496. 497. 498. 499. 500. 501. 502. 503. 504. 505. 506. 507. 508. 509. 510. 511. 512. 513. 514. 515. 516. 517. 518. 519. 520. 521. 522. 523. 524. 525. 526. 527. 528. 529. 530. 531. 532. 533. 534. 535. 536. 537. 538. 539. 540. 541. 542. 543. 544. 545. 546. 547. 548. 549. 550. 551. 552. 553. 554. 555. 556. 557. 558. 559. 560. 561. 562. 563. 564. 565. 566. 567. 568. 569. 570. 571. 572. 573. 574. 575. 576. 577. 578. 579. 580. 581. 582. 583. 584. 585. 586. 587. 588. 589. 590. 591. 592. 593. 594. 595. 596. 597. 598. 599. 600. 601. 602. 603. 604. 605. 606. 607. 608. 609. 610. 611. 612. 613. 614. 615. 616. 617. 618. 619. 620. 621. 622. 623. 624. 625. 626. 627. 628. 629. 630. 631. 632. 633. 634. 635. 636. 637. 638. 639. 640. 641. 642. 643. 644. 645. 646. 647. 648. 649. 650. 651. 652. 653. 654. 655. 656. 657. 658. 659. 660. 661. 662. 663. 664. 665. 666. 667. 668. 669. 670. 671. 672. 673. 674. 675. 676. 677. 678. 679. 680. 681. 682. 683. 684. 685. 686. 687. 688. 689. 690. 691. 692. 693. 694. 695. 696. 697. 698. 699. 700. 701. 702. 703. 704. 705. 706. 707. 708. 709. 710. 711. 712. 713. 714. 715. 716. 717. 718. 719. 720. 721. 722. 723. 724. 725. 726. 727. 728. 729. 730. 731. 732. 733. 734. 735. 736. 737. 738. 739. 740. 741. 742. 743. 744. 745. 746. 747. 748. 749. 750. 751. 752. 753. 754. 755. 756. 757. 758. 759. 760. 761. 762. 763. 764. 765. 766. 767. 768. 769. 770. 771. 772. 773. 774. 775. 776. 777. 778. 779. 780. 781. 782. 783. 784. 785. 786. 787. 788. 789. 790. 791. 792. 793. 794. 795. 796. 797. 798. 799. 800. 801. 802. 803. 804. 805. 806. 807. 808. 809. 810. 811. 812. 813. 814. 815. 816. 817. 818. 819. 820. 821. 822. 823. 824. 825. 826. 827. 828. 829. 830. 831. 832. 833. 834. 835. 836.

| 4 | 9 | 5 | 15 | 1 | 3 | 7 | 14 | 2 | 11 | 13 | 8 | 6 | 10 | 12 |
|---|---|---|----|---|---|---|----|---|----|----|---|---|----|----|
| h | k | a | a | y | i | t | y | g | d | m | t | r | o | t |
| t | c | g | e | n | a | o | s | d | n | y | h | p | i | o |
| d | r | u | e | n | g | o | i | t | t | a | e | x | s | t |
| r | s | i | l | e | n | e | x | e | i | g | i | t | v | n |
| a | a | t | c | r | b | e | k | a | i | s | | | | |

5. Cifrorul retranscrie coloanile în şiruri orizontale

6. Sursa de cofinanțare: Proiect finanțat prin grupuri de cercetare

YNNER GDTEA IACAB HTDRA AGUIT RPXTT OF - ET
LEKOC RLAOI SVLNT ITOT MLAG SYSEX KACOL C

Decodarea este procesul invers al cifrării, criptanaliza
 trebuind să determine mesajul original de transpoziție pe care

a putea ști cit de mari sînt coloanele. Acest fapt se poate obține împărțind numărul total al Literei la numărul literelor din chenar. În cazul nostru 71 la 14. Se obțin astfel 4 rînduri complete și un rînd incomplet de 11 litere.

Soluționarea unui singur număr cifrat prin transpoziție poate fi o problemă extrem de grea. Pentru a ne da seama de această exemplificăm cu ajutorul unei transpoziții simple. Criptanalistul va începe prin a separa criptograma în coloane și consideră el că ar putea fi un mesaj aplicare secvențele între ele până găsește două care ar putea sta unul lângă altul în tabelul original.

Să luăm o criptogramă de 40 de litere. Criptanalistul prezintă ea cheia este foarte simplă, de exemplu Căpănel va fi (Căpănel) din opt litere, el va împărți criptograma în grupe de câte opt litere și va împerechea primul grup cu celălalte patru :

| | | | | | | | |
|-----|-----|-----|-----|-----|-----|-----|-----|
| 1-2 | 1-3 | 1-4 | 1-5 | 2-1 | 3-1 | 4-1 | 5-1 |
| EN | EY | EM | EE | NE | YE | ME | EE |
| IH | IT | IR | IT | HI | TI | RI | TI |
| TE | TR | TH | TI | ET | RT | HT | IT |
| TG | TS | TI | TE | GT | ST | IT | ET |
| IR | IG | IN | IB | RI | GI | NI | BI |
| GN | GP | GU | GI | NG | PG | UG | IG |
| MM | MN | MU | MA | MM | NM | UM | AM |
| IT | IN | IO | II | TI | NI | OI | II |

Aceste coloane pot fi analizate atât din vedere cit și cu ajutorul diferențelor normale, care permite pentru a vedea care coloană merge cel mai bine. O metoda constă în a calcula frecvența fiecărei coloane dintr-un text clar, după care se face suma lor. Comparând aceste sume notând cel mai mare este foarte probabil să găsim cea bună. Astfel, EN, din impen-

recheres 1—2 are o frecvență normală de 25 o (din 26 o de
 73, 143, 77, 77, 73, 62 și 78. Criptanalistul va alege deci,
 1—4 cu totalul 143, apoi încearcă să extindă bigramele
 grame atât la stînga cit și la dreapta, prin aceeași metodă
 cînd reconstituie întregul tabel.

Dacă rezultatul este nesatisfăcător, modifică prez
 originală și începe de la început întreaga operație.

Acest tip de reconstrucție este posibil numai în cazuri
 excepționale pentru transpoziții duble. În teorie, criptanalistul
 trebuie să construiască coloanele celui de-al doilea tabel și să
 ale bigramele și trigramele care să se transforme în text clar

grame de aceeași lungime și cifrate cu aceeași cheie. Criptana-
 mări multiple folosită pentru cuvinte. De obicei, cele două
 mesaje sînt scrise unul sub altul pe linii de hîrtie, iar hîrtia este
 tăiată vertical, astfel încît două litere — cîte una din fiecare

frunzele toamna.

sau grătar. Grătarul nărilor — cel mai des folosit —
 este un pătrat de hîrtie sau carton împărțit în câmpuri dre-
 care sunt decupate. Împărțirea se face astfel încît să
 a fost așezat pe hîrtie și apoi pe un pătrat de
 casuțele din pătrat și din restul său pătrat se
 locurile și se scrie în fiecare din ele o literă

transmis.

Cînd toate casuțele din cel de-al doilea pătrat de hîrtie au
 fost completate, criptograful le poate transmite, citindu-le, de
 obicei, pe rînduri. Mesaje mai lungi se cifrează repetînd ope-
 rația, iar dacă rămîn casuțe goale, acestea se pot șterge sau
 umple cu nule.

Nemții au dat trupelor lor grătare de diferite mărimi. Fie-
 care avea un nume codificat după cum urmează: Anna —
 grătarul de 25, Berta — grătarul de 36, Clara — grătarul de
 49, Dora — grătarul de 64, Emil — grătarul de 81 și Franz —
 grătarul de 100. Aceste nume codificate se schimbau săptămînal.

În aceste procedee pentru a le soluționa

na la nu permite închiderea circuitului, iar curentul electric nu trece prin electromagnet. Ca atare, hirtia rămâne intactă.

Vernam a sugerat ca pe o bandă de hirtie să fie transmise o cheie formată din semne și spații, care să se adune, în mod electric, cu impulsurile textului clar, suma urmând să constituie impulsurile textului cifrat, suma urmând să constituie impulsurile textului clar. Vernam a stat pe această idee și a sugerat ca impulsurile textului cifrat să fie transmise pe o bandă separată de hirtie. Dacă impulsul cheii este un impuls și impulsul textului clar este un impuls, atunci suma celor doi impulsuri va fi un impuls sau un spațiu, în funcție de valoarea sumei. Dacă suma este 1 sau 0, atunci impulsul va fi un impuls sau un spațiu, în funcție de valoarea sumei. Dacă suma este 1 sau 0, atunci impulsul va fi un impuls sau un spațiu, în funcție de valoarea sumei. Dacă suma este 1 sau 0, atunci impulsul va fi un impuls sau un spațiu, în funcție de valoarea sumei.

| text clar | cheie | text cifrat |
|-----------|-------|-------------|
| semn | + | spațiu |
| semn | + | semn |
| spațiu | + | semn |
| spațiu | + | spațiu |

De exemplu, dacă textul clar este "11000" și cheia este "10011", atunci textul cifrat va fi "01011".

Intregul sistem poate fi aranjat într-un singur tabel. Folosind simbolurile 1 pentru semn și 0 pentru spațiu, regula poate fi exprimată astfel:

| text clar | cheie | text cifrat |
|-----------|-------|-------------|
| 1 | 0 | 1 |
| 0 | 1 | 0 |

Conform cu această regulă, Vernam a combinat cele cinci unități ale caracterelor clare cu cele ale cheii și a obținut cinci unități de caractere cifrate. Astfel, dacă textul clar este 1 sau 11000, iar cheia este 10011, textul cifrat este următorul:

text clar : 11000
cheie : 10011
text cifrat : 01011

Textul clar obținut de corespondent a rezultat din combinarea care a avut loc prin aplicarea impulsurilor care constituie cheia pe te impulsurile textului clar. De exemplu, dacă textul clar = 10100, cheia = 01111, atunci:

text cifrat : 11011
cheie : 01111
text clar : 10100

Ca să combine electric impulsurile, Vernam a inventat un aparat din magneti, relee și bobine. Cum cifrarea și decifrarea erau reciproce, aparatul era folosit atât pentru ambele operațiuni.

Aparatul era introdus într-o bandă de hirtie pe care era scrisă cheia. Când aparatul era pus în funcțiune, pe ecran apareau impulsurile textului cifrat și apărea un impuls pentru fiecare impuls al textului clar și apărea un impuls pentru fiecare impuls al cheii. Astfel, se putea vedea că orice alt mesaj trimis, la corespondent, unde aparatul Vernam era folosit, se putea decifra cu cheia scrisă pe banda expeditorului și astfel se obținea textul clar. Automat, banda de hirtie se transmitea la corespondent și, în felul acesta, se obținea mesajul direct în clar.

Într-un alt aparat, Vernam a folosit o bandă de hirtie pe care era scrisă cheia. Când aparatul era pus în funcțiune, pe ecran apareau impulsurile textului cifrat și apărea un impuls pentru fiecare impuls al textului clar și apărea un impuls pentru fiecare impuls al cheii. Astfel, se putea vedea că orice alt mesaj trimis, la corespondent, unde aparatul Vernam era folosit, se putea decifra cu cheia scrisă pe banda expeditorului și astfel se obținea textul clar. Automat, banda de hirtie se transmitea la corespondent și, în felul acesta, se obținea mesajul direct în clar.

De exemplu, dacă textul clar este 11000 și cheia este 10011, atunci textul cifrat este 01011.

volat rapid. În primele zile cheile pentru acest aparat aveau forma unor rotoare cu benzi de hârtie pe care erau imprimate semne trase din pălărie, colorându-se astfel chei întâmplătoare. Dar inginerii care au inventat repede criptologie, și-au dat seama de faptul că acesta nu putea fi un sistem științific și au făcut o asemănare între aceste sisteme polialfabetice. Cu ajutorul codului Baudot, se poate forma un tablou de 32×32 în care se poate deosebi prin sărituri clar, iar prima cheie este cheia.

Intrucât secretul sistemului lui Vernam rezida mai ales în cheile care erau la fel ca cele ale lui Baudot, dar erau foarte lungi care, pentru a fi schimbate, trebuiau să fie înlocuite în mod inconvenient. Într-un sensul că benzile erau greu de manipulat. De aceea, un alt inventator, Albert Hill, a găsit la combaterea acestor chei scurte într-un aparat Vernam, ca și cum una ar fi servit la cifrarea celeilalte. Rezultatul obținut: o bandă foarte lungă care servea drept cheie pentru textul clar. Acest tip de cheie s-a numit cheie secundară. Lungunea ei provenea din diferența de semne din cheile primare. De exemplu, dacă cele două chei primare înregistrate conțineau una 1 000 de caractere, iar cealaltă 999, diferența de un singur caracter dădea naștere la 999 000 de combinații. Astfel, două benzi de aproximativ 4 m fiecare dădeau naștere unei chei care, pentru a putea fi înregistrată, erau necesari peste 4 000 metri de bandă. Aceasta a fost una din cele mai de seamă îmbunătățiri.

Totuși, nici acest sistem nu putea fi considerat ca impenetrabil în fața criptanalizatorilor căci orice repetare, de orice fel, a cheii

permitea descoperirea textului clar. Se poate spune că în

acest sistem, cheia este o singură dată și nu se repetă.

Într-un alt sistem, cheia este o singură dată și nu se repetă.

Într-un alt sistem, cheia este o singură dată și nu se repetă.

Într-un alt sistem, cheia este o singură dată și nu se repetă.

Într-un alt sistem, cheia este o singură dată și nu se repetă.

asta. Așa s-a născut cheia filată o singură dată. Căci, în acest sistem, cheia este o singură dată și nu se repetă. Acest fapt este foarte important pentru fiecare mesaj dintr-un grup de corespondență.

Un astfel de sistem nu poate fi folosit decât în

cazul în care, indiferent de lungimea de text și de timp pe

care se folosește, analiza este la fel de ușoară ca și la o cheie

care servește ca cheie pentru textul clar. În acest sens, există mai

multe sisteme. Una dintre ele este sistemul Kerckhoffs care constă

în folosirea literelor care sunt încheiate cu o cheie

care este o singură dată și nu se repetă. Într-un text clar, se

poate folosi o cheie care este o singură dată și nu se repetă.

Într-un text clar, se poate folosi o cheie care este o singură dată

și nu se repetă. Într-un text clar, se poate folosi o cheie care

este o singură dată și nu se repetă. Într-un text clar, se poate

folosi o cheie care este o singură dată și nu se repetă. Într-un

text clar, se poate folosi o cheie care este o singură dată și nu

se repetă. Într-un text clar, se poate folosi o cheie care este

o singură dată și nu se repetă. Într-un text clar, se poate

folosi o cheie care este o singură dată și nu se repetă. Într-un

text clar, se poate folosi o cheie care este o singură dată și nu

Dar mai exista te na p. habilitatilor, calculul este
S-ar putea ca intrucat de la a tuturor cheilor posibile, se
dupa asta ar putea da o lista cu textul clar Succesul obtinut pe
aceasta cale este mult mai mic decat cel al metodei foarte grea sa adugim
noul de la fiecare litera din mesaj, descoperind prin aceasta
parola pentru textul clar sau pe termen lung un criptanalist care
trebuie sa lucreze cu toate literele, luind la rand
cele posibile pentru fiecare litera. Textul clar obtinut cu cheia
AABI ar fi kiss (sarut). Nu este cel cautat. Merge mai departe
AAEL da kill (a ucide). Incepe sa fie pe drumul cel bun dar
vreca sa fie sigur si continua. Cheia AAEM da kilt (fusta de
hoie), AAEI da kil (candida) sau o referire la o manevra a
scotlenilor. AAER da kiln (cuzan de țuică). Obține apoi
tele fast (repede) cu cheia LZBM, slow (incet) cu KHIA, stop
cu LHMV, etc. Pentru a afla ce este K-7T, răsfoiește în

1. $x + 2$ sau $4 + 5$ ori al orărilor, altele decât cele 12 de
 ore, este posibil. Generalizând, pentru ecuația $x + y = 0$
 există o ecuație cu două necunoscute care are infinite soluții
 reale. Dacă ecuația cu două necunoscute are infinite soluții
 reale, înlocuim o singură oră cu o altă oră, și tot așa
 până la sfârșit. Din cele două ecuații rezultă că în orice
 caz din cazul 1) rezultă că în orice oră există cel puțin
 un tren. Altfel, s-ar afla că în orice oră există cel puțin
 un tren care nu este în stație, ceea ce este imposibil.
 În concluzie, în orice oră există cel puțin un tren în stație.
 Dacă în orice oră există cel puțin un tren în stație, atunci
 din orice stație există cel puțin un tren în stație.
 Dacă în orice oră există cel puțin un tren în stație, atunci
 din orice stație există cel puțin un tren în stație.

de la 0 la 25, orice număr mai mare decât 25 trebuie redus modulo 26. Astfel, 28 este congruent cu 2 modulo 26 deoarece $28 - 26 = 2$. La fel 68 este congruent 16, modulo 26, deoarece $68 - 26 - 2$, rest 16.

Pentru a demonstra cum funcționează sistemul inventat de el, Hill a înlocuit literele textului clar cu x , iar literele textului cifrat cu y în ordinea x_1 — prima literă, x_2 cea de-a doua ș.a.m.d. A ajuns, astfel, la următoarele ecuații:

$$y_1 = 8x_1 + 6x_2 + 9x_3 + 5x_4$$

$$y_2 = 6x_1 + 9x_2 + 5x_3 + 10x_4$$

$$y_3 = 5x_1 + 8x_2 + 4x_3 + 9x_4$$

$$y_4 = 10x_1 + 6x_2 + 11x_3 + 4x_4$$

Cînd a început cifrarea unui text ca acesta: „Delay operations” (întîrziată operațiunile — N.T.), Hill a transformat literele din textul clar în numere luate la întimplare, ca în exemplul de mai jos:

| | | | | | | | | | | | | | | | | | | | |
|----|----|----|----|----|----|---|---|----|----|---|----|----|---|---|---|----|---|----|----|
| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t |
| 5 | 23 | 2 | 20 | 10 | 15 | 8 | 4 | 18 | 25 | 0 | 16 | 13 | 7 | 3 | 1 | 19 | 6 | 12 | 24 |
| u | v | w | x | y | z | | | | | | | | | | | | | | |
| 21 | 17 | 14 | 22 | 11 | 9 | | | | | | | | | | | | | | |

Apoi a luat valorile numerice ale primelor patru litere din textul clar, în cazul nostru „dela”, și le-a trecut în locul lui x_1 , x_2 , x_3 , x_4 din ecuațiile de mai sus. Procedînd astfel, a ajuns la următoarea formulă:

$$y_1 = (8 \times 20) + (6 \times 10) + (9 \times 16) + (5 \times 5)$$

$$y_2 = (6 \times 20) + (9 \times 10) + (5 \times 16) + (10 \times 5)$$

$$y_3 = (5 \times 20) + (8 \times 10) + (4 \times 16) + (9 \times 5)$$

$$y_4 = (10 \times 20) + (6 \times 10) + (11 \times 16) + (4 \times 5)$$

În continuare Hill a făcut înmulțirile și adunările aplicînd regula modulo 26. De exemplu, cînd a rezolvat pe y_1 a obținut: $8 \times 20 = 160$; $160 : 26 = 6$, rest 4. Deci $8 \times 20 = 4$; la fel a făcut toate celelalte operații $6 \times 10 = 8$, $9 \times 16 = 14$ și $5 \times 5 = 25$.

Fiind dat final al adunării este 51. Deci aplicînd modulo 26 obținem 25, care, în alfabetul nostru este egal cu litera „z”. Cele litere sînt afișate în alfabetul nostru astfel: „dela” devine JCOW, iar textul cifrat devine ZYAPDVLEQVNC.

Să presupunem că textul clar este „dela” și textul cifrat este ZYAPDVLEQVNC. Dacă aplicăm modulo 26 la fiecare literă din textul cifrat, obținem: Z=25, Y=24, A=1, P=15, D=4, V=22, L=12, E=5, Q=17, V=22, N=13, C=3. Aceste numere sînt valorile numerice ale literelor din textul cifrat. Pentru a descifra textul, trebuie să găsim valorile numerice ale literelor din textul clar. Pentru aceasta trebuie să rezolvăm sistemul de ecuații:

Valorile fixe în ecuații — numerele cu care se înmulțesc numerele literelor din textul clar — nu pot fi selecționate la întimplare, ci trebuie să fie numerele care sînt înlocuite în ecuații. Pentru cazul nostru, aceste ecuații sînt:

$$x_1 = 23y_1 + 20y_2 + 5y_3 + 1y_4$$

$$x_2 = 2y_1 + 11y_2 + 18y_3 + 1y_4$$

$$x_3 = 2y_1 + 20y_2 + 6y_3 + 25y_4$$

$$x_4 = 25y_1 + 2y_2 + 22y_3 + 23y_4$$

Hill a eliminat însă în cele din urmă ecuațiile de descriere, cînd, transformînd ecuațiile, a obținut următoarea ecuație care servește atât la cifrare cît și la descifrare. Aceste „transformări involutorii” sînt construite cu ajutorul unei formule speciale, care limitează numărul ecuațiilor. În acest caz este faptul că ecuațiile sînt de gradul 1, ceea ce înseamnă că reducerea este posibilă. Astfel, ecuațiile pot fi reduse la o singură ecuație, care este de gradul 1, cu proporția în care ne ușurează operațiunea.

Operațiunea de cifrare a fost ușurată și mai mult prin introducerea matricei. O matrice este o tabelă în care sînt scrise numere. Matricele pot fi de orice dimensiune, dar trebuie să fie pătrate, iar numerele sînt scrise în proporția în care

sate 26 de contacte electrice, așezate la distanțe egale. Aceste contacte sînt, de regulă, fabricate din aramă sau alamă. Fiecare contact este legat la intrare cu un contact de pe partea opusă, astfel încît se stabilește o legătură electrică între două puncte opuse situate pe o circumferință. Contactele de la intrare, cînd rotorul, în rotor formarea literelor textului clar, iar contactele de la ieșire, literelor textului cifrat. Firul electric care le unește de la o parte la alta asigură transformarea literelor textului clar în text cifrat.

Pentru a cifra un mesaj se conectează o sursă de curent electric la rotor, la contactul de intrare a literei pe care vrem să o cifrăm, să zicem *a*. Curentul trece de-a lungul firului și ajunge la contactul de pe partea opusă, care reprezintă, să zicem, litera *R*. Dacă se face o listă cu toate legăturile de pe cele două părți, se obține un alfabet de substituție simplă. În felul acesta, rotorul conține un alfabet de cifrat sub o formă care se pretează la manipulare electromecanică.

Pentru a se putea executa o asemenea manipulare, rotorul este montat pe o placă de material izolant și avînd 26 de contacte fixate sub formă de cerc, în așa fel încît să se potrivească cu cele de pe rotor. Fiecare contact de pe placa de intrare a curentului este conectat la litera unei mașini de scris care reprezintă litera textului clar. Contactele de pe placa de ieșire sînt conectate la un tablou pe care, cu ajutorul unui beculeț, se indică litera din textul cifrat. Cînd cifrorul apasă pe cheia ce reprezintă litera *a*, el stabilește o legătură electrică între contactul de la sursă la primul contact pe care este montat rotorul la contactul literei *a* și la contactul literei *R* de pe partea opusă, adică la contactul care reprezintă litera *R* cifrat pe placa de ieșire. Astfel, contactele rotorului transformă litera *R* de pe tabloul de ieșire în litera *a* de pe tabloul de intrare.

Dacă rotorul se rotește o dată, această altitudine, integrală a rotorului, se schimbă și astfel se schimbă și alfabetul de substituție. În practică însă, rotorul nu se rotește o dată, ci se rotește cu o fracțiune dintr-o rotație completă. Astfel, se poate spune că se naște o nouă alfabet de substituție pentru fiecare literă *a*, de exemplu.

Alfabetul de substituție este astfel: *P* *a* *b* *c* *d* *e* *f* *g* *h* *i* *j* *k* *l* *m* *n* *o* *p* *q* *r* *s* *t* *u* *v* *w* *x* *y* *z*. Dacă rotorul se rotește o dată, alfabetul de substituție devine: *P* *a* *b* *c* *d* *e* *f* *g* *h* *i* *j* *k* *l* *m* *n* *o* *p* *q* *r* *s* *t* *u* *v* *w* *x* *y* *z*. Dacă rotorul se rotește o dată, alfabetul de substituție devine: *P* *a* *b* *c* *d* *e* *f* *g* *h* *i* *j* *k* *l* *m* *n* *o* *p* *q* *r* *s* *t* *u* *v* *w* *x* *y* *z*. Dacă rotorul se rotește o dată, alfabetul de substituție devine: *P* *a* *b* *c* *d* *e* *f* *g* *h* *i* *j* *k* *l* *m* *n* *o* *p* *q* *r* *s* *t* *u* *v* *w* *x* *y* *z*. Dacă rotorul se rotește o dată, alfabetul de substituție devine: *P* *a* *b* *c* *d* *e* *f* *g* *h* *i* *j* *k* *l* *m* *n* *o* *p* *q* *r* *s* *t* *u* *v* *w* *x* *y* *z*. Dacă rotorul se rotește o dată, alfabetul de substituție devine: *P* *a* *b* *c* *d* *e* *f* *g* *h* *i* *j* *k* *l* *m* *n* *o* *p* *q* *r* *s* *t* *u* *v* *w* *x* *y* *z*. Dacă rotorul se rotește o dată, alfabetul de substituție devine: *P* *a* *b* *c* *d* *e* *f* *g* *h* *i* *j* *k* *l* *m* *n* *o* *p* *q* *r* *s* *t* *u* *v* *w* *x* *y* *z*. Dacă rotorul se rotește o dată, alfabetul de substituție devine: *P* *a* *b* *c* *d* *e* *f* *g* *h* *i* *j* *k* *l* *m* *n* *o* *p* *q* *r* *s* *t* *u* *v* *w* *x* *y* *z*. Dacă rotorul se rotește o dată, alfabetul de substituție devine: *P* *a* *b* *c* *d* *e* *f* *g* *h* *i* *j* *k* *l* *m* *n* *o* *p* *q* *r* *s* *t* *u* *v* *w* *x* *y* *z*. Dacă rotorul se rotește o dată, alfabetul de substituție devine: *P* *a* *b* *c* *d* *e* *f* *g* *h* *i* *j* *k* *l* *m* *n* *o* *p* *q* *r* *s* *t* *u* *v* *w* *x* *y* *z*. Dacă rotorul se rotește o dată, alfabetul de substituție devine: *P* *a* *b* *c* *d* *e* *f* *g* *h* *i* *j* *k* *l* *m* *n* *o* *p* *q* *r* *s* *t* *u* *v* *w* *x* *y* *z*. Dacă rotorul se rotește o dată, alfabetul de substituție devine: *P* *a* *b* *c* *d* *e* *f* *g* *h* *i* *j* *k* *l* *m* *n* *o* *p* *q* *r* *s* *t* *u* *v* *w* *x* *y* *z*. Dacă rotorul se rotește o dată, alfabetul de substituție devine: *P* *a* *b* *c* *d* *e* *f* *g* *h* *i* *j* *k* *l* *m* *n* *o* *p* *q* *r* *s* *t* *u* *v* *w* *x* *y* *z*. Dacă rotorul se rotește o dată, alfabetul de substituție devine: *P* *a* *b* *c* *d* *e* *f* *g* *h* *i* *j* *k* *l* *m* *n* *o* *p* *q* *r* *s* *t* *u* *v* *w* *x* *y* *z*. Dacă rotorul se rotește o dată, alfabetul de substituție devine: *P* *a* *b* *c* *d* *e* *f* *g* *h* *i* *j* *k* *l* *m* *n* *o* *p* *q* *r* *s* *t* *u* *v* *w* *x* *y* *z*. Dacă rotorul se rotește o dată, alfabetul de substituție devine: *P* *a* *b* *c* *d* *e* *f* *g* *h* *i* *j* *k* *l* *m* *n* *o* *p* *q* *r* *s* *t* *u* *v* *w* *x* *y* *z*. Dacă rotorul se rotește o dată, alfabetul de substituție devine: *P* *a* *b* *c* *d* *e* *f* *g* *h* *i* *j* *k* *l* *m* *n* *o* *p* *q* *r* *s* *t* *u* *v* *w* *x* *y* *z*. Dacă rotorul se rotește o dată, alfabetul de substituție devine: *P* *a* *b* *c* *d* *e* *f* *g* *h* *i* *j* *k* *l* *m* *n* *o* *p* *q* *r* *s* *t* *u* *v* *w* *x* *y* *z*. Dacă rotorul se rotește o dată, alfabetul de substituție devine: *P* *a* *b* *c* *d* *e* *f* *g* *h* *i* *j* *k* *l* *m* *n* *o* *p* *q* *r* *s* *t* *u* *v* *w* *x* *y* *z*. Dacă rotorul se rotește o dată, alfabetul de substituție devine: *P* *a* *b* *c* *d* *e* *f* *g* *h* *i* *j* *k* *l* *m* *n* *o* *p* *q* *r* *s* *t* *u* *v* *w* *x* *y* *z*. Dacă rotorul se rotește o dată, alfabetul de substituție devine: *P* *a* *b* *c* *d* *e* *f* *g* *h* *i* *j* *k* *l* *m* *n* *o* *p* *q* *r* *s* *t* *u* *v* *w* *x* *y* *z*. Dacă rotorul se rotește o dată, alfabetul de substituție devine: *P* *a* *b* *c* *d* *e* *f* *g* *h* *i* *j* *k* *l* *m* *n* *o* *p* *q* *r* *s* *t* *u* *v* *w* *x* *y* *z*. Dacă rotorul se rotește o dată, alfabetul de substituție devine: *P* *a* *b* *c* *d* *e* *f* *g* *h* *i* *j* *k* *l* *m* *n* *o* *p* *q* *r* *s* *t* *u* *v* *w* *x* *y* *z*. Dacă rotorul se rotește o dată, alfabetul de substituție devine: *P* *a* *b* *c* *d* *e* *f* *g* *h* *i* *j* *k* *l* *m* *n* *o* *p* *q* *r* *s* *t* *u* *v* *w* *x* *y* *z*. Dacă rotorul se rotește o dată, alfabetul de substituție devine: *P* *a* *b* *c* *d* *e* *f* *g* *h* *i* *j* *k* *l* *m* *n* *o* *p* *q* *r* *s* *t* *u* *v* *w* *x* *y* *z*. Dacă rotorul se rotește o dată, alfabetul de substituție devine: *P* *a* *b* *c* *d* *e* *f* *g* *h* *i* *j* *k* *l* *m* *n* *o* *p* *q* *r* *s* *t* *u* *v* *w* *x* *y* *z*. Dacă rotorul se rotește o dată, alfabetul de substituție devine: *P* *a* *b* *c* *d* *e* *f* *g* *h* *i* *j* *k* *l* *m* *n* *o* *p* *q* *r* *s* *t* *u* *v* *w* *x* *y* *z*. Dacă rotorul se rotește o dată, alfabetul de substituție devine: *P* *a* *b* *c* *d* *e* *f* *g* *h* *i* *j* *k* *l* *m* *n* *o* *p* *q* *r* *s* *t* *u* *v* *w* *x* *y* *z*. Dacă rotorul se rotește o dată, alfabetul de substituție devine: *P* *a* *b* *c* *d* *e* *f* *g* *h* *i* *j* *k* *l* *m* *n* *o* *p* *q* *r* *s* *t* *u* *v* *w* *x* *y* *z*. Dacă rotorul se rotește o dată, alfabetul de substituție devine: *P* *a* *b* *c* *d* *e* *f* *g* *h* *i* *j* *k* *l* *m* *n* *o* *p* *q* *r* *s* *t* *u* *v* *w* *x* *y* *z*. Dacă rotorul se rotește o dată, alfabetul de substituție devine: *P* *a* *b* *c* *d* *e* *f* *g* *h* *i* *j* *k* *l* *m* *n* *o* *p* *q* *r* *s* *t* *u* *v* *w* *x* *y* *z*. Dacă rotorul se rotește o dată, alfabetul de substituție devine: *P* *a* *b* *c* *d* *e* *f* *g* *h* *i* *j* *k* *l* *m* *n* *o* *p* *q* *r* *s* *t* *u* *v* *w* *x* *y* *z*. Dacă rotorul se rotește o dată, alfabetul de substituție devine: *P* *a* *b* *c* *d* *e* *f* *g* *h* *i* *j* *k* *l* *m* *n* *o* *p* *q* *r* *s* *t* *u* *v* *w* *x* *y* *z*. Dacă rotorul se rotește o dată, alfabetul de substituție devine: *P* *a* *b* *c* *d* *e* *f* *g* *h* *i* *j* *k* *l* *m* *n* *o* *p* *q* *r* *s* *t* *u* *v* *w* *x* *y* *z*. Dacă rotorul se rotește o dată, alfabetul de substituție devine: *P* *a* *b* *c* *d* *e* *f* *g* *h* *i* *j* *k* *l* *m* *n* *o* *p* *q* *r* *s* *t* *u* *v* *w* *x* *y* *z*. Dacă rotorul se rotește o dată, alfabetul de substituție devine: *P* *a* *b* *c* *d* *e* *f* *g* *h* *i* *j* *k* *l* *m* *n* *o* *p* *q* *r* *s* *t* *u* *v* *w* *x* *y* *z*. Dacă rotorul se rotește o dată, alfabetul de substituție devine: *P* *a* *b* *c* *d* *e* *f* *g* *h* *i* *j* *k* *l* *m* *n* *o* *p* *q* *r* *s* *t* *u* *v* *w* *x* *y* *z*. Dacă rotorul se rotește o dată, alfabetul de substituție devine: *P* *a* *b* *c* *d* *e* *f* *g* *h* *i* *j* *k* *l* *m* *n* *o* *p* *q* *r* *s* *t* *u* *v* *w* *x* *y* *z*. Dacă rotorul se rotește o dată, alfabetul de substituție devine: *P* *a* *b* *c* *d* *e* *f* *g* *h* *i* *j* *k* *l* *m* *n* *o* *p* *q* *r* *s* *t* *u* *v* *w* *x* *y* *z*. Dacă rotorul se rotește o dată, alfabetul de substituție devine: *P* *a* *b* *c* *d* *e* *f* *g* *h* *i* *j* *k* *l* *m* *n* *o* *p* *q* *r* *s* *t* *u* *v* *w* *x* *y* *z*. Dacă rotorul se rotește o dată, alfabetul de substituție devine: *P* *a* *b* *c* *d* *e* *f* *g* *h* *i* *j* *k* *l* *m* *n* *o* *p* *q* *r* *s* *t* *u* *v* *w* *x* *y* *z*. Dacă rotorul se rotește o dată, alfabetul de substituție devine: *P* *a* *b* *c* *d* *e* *f* *g* *h* *i* *j* *k* *l* *m* *n* *o* *p* *q* *r* *s* *t* *u* *v* *w* *x* *y* *z*. Dacă rotorul se rotește o dată, alfabetul de substituție devine: *P* *a* *b* *c* *d* *e* *f* *g* *h* *i* *j* *k* *l* *m* *n* *o* *p* *q* *r* *s* *t* *u* *v* *w* *x* *y* *z*. Dacă rotorul se rotește o dată, alfabetul de substituție devine: *P* *a* *b* *c* *d* *e* *f* *g* *h* *i* *j* *k* *l* *m* *n* *o* *p* *q* *r* *s* *t* *u* *v* *w* *x* *y* *z*. Dacă rotorul se rotește o dată, alfabetul de substituție devine: *P* *a* *b* *c* *d* *e* *f* *g* *h* *i* *j* *k* *l* *m* *n* *o* *p* *q* *r* *s* *t* *u* *v* *w* *x* *y* *z*. Dacă rotorul se rotește o dată, alfabetul de substituție devine: *P* *a* *b* *c* *d* *e* *f* *g* *h* *i* *j* *k* *l* *m* *n* *o* *p* *q* *r* *s* *t* *u* *v* *w* *x* *y* *z*. Dacă rotorul se rotește o dată, alfabetul de substituție devine: *P* *a* *b* *c* *d* *e* *f* *g* *h* *i* *j* *k* *l* *m* *n* *o* *p* *q* *r* *s* *t* *u* *v* *w* *x* *y* *z*. Dacă rotorul se rotește o dată, alfabetul de substituție devine: *P* *a* *b* *c* *d* *e* *f* *g* *h* *i* *j* *k* *l* *m* *n* *o* *p* *q* *r* *s* *t* *u* *v* *w* *x* *y* *z*. Dacă rotorul se rotește o dată, alfabetul de substituție devine: *P* *a* *b* *c* *d* *e* *f* *g* *h* *i* *j* *k* *l* *m* *n* *o* *p* *q* *r* *s* *t* *u* *v* *w* *x* *y* *z*. Dacă rotorul se rotește o dată, alfabetul de substituție devine: *P* *a* *b* *c* *d* *e* *f* *g* *h* *i* *j* *k* *l* *m* *n* *o* *p* *q* *r* *s* *t* *u* *v* *w* *x* *y* *z*. Dacă rotorul se rotește o dată, alfabetul de substituție devine: *P* *a* *b* *c* *d* *e* *f* *g* *h* *i* *j* *k* *l* *m* *n* *o* *p* *q* *r* *s* *t* *u* *v* *w* *x* *y* *z*. Dacă rotorul se rotește o dată, alfabetul de substituție devine: *P* *a* *b* *c* *d* *e* *f* *g* *h* *i* *j* *k* *l* *m* *n* *o* *p* *q* *r* *s* *t* *u* *v* *w* *x* *y* *z*. Dacă rotorul se rotește o dată, alfabetul de substituție devine: *P* *a* *b* *c* *d* *e* *f* *g* *h* *i* *j* *k* *l* *m* *n* *o* *p* *q* *r* *s* *t* *u* *v* *w* *x* *y* *z*. Dacă rotorul se rotește o dată, alfabetul de substituție devine: *P* *a* *b* *c* *d* *e* *f* *g* *h* *i* *j* *k* *l* *m* *n* *o* *p* *q* *r* *s* *t* *u* *v* *w* *x* *y* *z*. Dacă rotorul se rotește o dată, alfabetul de substituție devine: *P* *a* *b* *c* *d* *e* *f* *g* *h* *i* *j* *k* *l* *m* *n* *o* *p* *q* *r* *s* *t* *u* *v* *w* *x* *y* *z*. Dacă rotorul se rotește o dată, alfabetul de substituție devine: *P* *a* *b* *c* *d* *e* *f* *g* *h* *i* *j* *k* *l* *m* *n* *o* *p* *q* *r* *s* *t* *u* *v* *w* *x* *y* *z*. Dacă rotorul se rotește o dată, alfabetul de substituție devine: *P* *a* *b* *c* *d* *e* *f* *g* *h* *i* *j* *k* *l* *m* *n* *o* *p* *q* *r* *s* *t* *u* *v* *w* *x* *y* *z*. Dacă rotorul se rotește o dată, alfabetul de substituție devine: *P* *a* *b* *c* *d* *e* *f* *g* *h* *i* *j* *k* *l* *m* *n* *o* *p* *q* *r* *s* *t* *u* *v* *w* *x* *y* *z*. Dacă rotorul se rotește o dată, alfabetul de substituție devine: *P* *a* *b* *c* *d* *e* *f* *g* *h* *i* *j* *k* *l* *m* *n* *o* *p* *q* *r* *s* *t* *u* *v* *w* *x* *y* *z*. Dacă rotorul se rotește o dată, alfabetul de substituție devine: *P* *a* *b* *c* *d* *e* *f* *g* *h* *i* *j* *k* *l* *m* *n* *o* *p* *q* *r* *s* *t* *u* *v* *w* *x* *y* *z*. Dacă rotorul se rotește o dată, alfabetul de substituție devine: *P* *a* *b* *c* *d* *e* *f* *g* *h* *i* *j* *k* *l* *m* *n* *o* *p* *q* *r* *s* *t* *u* *v* *w* *x* *y* *z*. Dacă rotorul se rotește o dată, alfabetul de substituție devine: *P* *a* *b* *c* *d* *e* *f* *g* *h* *i* *j* *k* *l* *m* *n* *o* *p* *q* *r*

Acestea sunt principalele de bază ale soluționării sistemului rotor, dar, așa cum va puteți da seama, sistemul rotor produce totuși un cifrat extrem de complex și de rezistent.

Cei prima inventatori ai rotorului de cifrat au fost americanul Edward Hebern, olandezul Hugo Alexander Koch, germanul Arthur Scherbius și suedezul Arvid Gerhard Damm.

După cel de-al doilea război mondial, milionarul suedez Hagelin, unul dintre cei care au perfecționat mașina de cifrat, a pus bazele unei firme ce fabrică mașini de cifrat pe care le vinde pe piața internațională. Printre clienții săi se numără peste 60 de guverne din diferite țări, care cumpără aceste mașini atât pentru oficile diplomatice cit și pentru armată. Instalația completă costă între 30 000 și 50 000 de dolari, iar funcționarii firmei explică tuturor procedeele de funcționare a mașinilor, metodele de stabilire a cheilor, dar se feresc să facă recomandări precise, ca nu cumva clientul să creadă că ele se dau și la alții.

Din modul în care prosperă Hagelin, reiese clar că afacerile sînt rentabile și „secretul” constituie o afacere bănoasă.

CENZORI ȘI SPIONI

Cifrul este limba spionilor care, de obicei, vorbesc în șoaptă. Pentru ca acțiunile unui spion să fie încununate de succes este necesar ca el să nu fie văzut și auzit. Trimiterea de mesaje sub formă criptografică ar putea să fie văzută, dar șoapta spionului ar fi repede pecetluită. Totuși, el trebuie să transmită informațiile pe care le are, altfel existența sa nu este justificată. Așa se face că el recurge la metode subtile de a ascunde chiar și faptul că a fost trimis un mesaj secret. Pentru a bloca această posibilitate cit și pentru a descoperi dușmanul care a pătruns în interior, guvernele tuturor țărilor au construit filtre pentru a preveni și detecta comunicările secrete. Aceste filtre, care lasă să treacă numai mesajele nevinovate, nu sînt altele decît organele de cenzură.

În continuare, vor fi prezentate cîteva din metodele folosite de către spioni în comerțul cu informații secrete.

În special, în timp de război se impun o serie de restricții asupra corespondenței, pentru a preveni scurgerea de informații secrete de către corespondenți. Aceste restricții sînt de obicei aplicate prin corespondența prin intermediul unor metode de decupări, listări, etc. Motivele acestor restricții pot fi de multe feluri. Unele trimiteri pot asigura informații care sînt deosebit de importante. Un exemplu în acest sens este...

fi putut dovedi absolut necesar, îl constituie cazul reținerii unei scrisori în care se dădeau niște instrucțiuni de tricotat. Serviciul de cenzură american din timpul celui de-al doilea război mondial a reținut această scrisoare pînă cînd o funcționară din cadrul acestui serviciu a confecționat un pulover întreg urmînd instrucțiunile din scrisoare, pentru a vedea dacă în spatele lor nu se ascundea cu totul altceva. Un caz asemănător s-a întîmplat în timpul revoluției franceze, cînd o oarecare doamnă Deforge a „tricotat” numele mai multor dușmani ai republicii.

Scrisorile cu un text neclar, care conțin anumite cifre de afaceri ori care sînt scrise într-o limbă străină uzuală, sînt reținute.

Precauțiuni se iau și în ce privește anunțurile și reclamele. Ziarele sînt avertizate asupra pericolului de a publica anumite reclame sau anunțuri care conțin mesaje secrete. Măsuri speciale trebuie, de asemenea, luate în ceea ce privește posturile de radio, care pot transmite mesaje în cod deschis pentru spioni, submarine sau către centrele de spionaj străine. În Anglia și S.U.A. s-au interzis cu desăvîrșire în timpul celui de-al doilea război mondial transmiterea de interviuri cu oameni de pe stradă, liste de jucării pe care Moș Gerilă le dădea copiilor sau erau de vânzare, anunțuri despre pierderea unor cîini etc.

Aceasta este doar o parte din activitatea de cenzură, cealaltă parte se referă la detectarea altor metode care ar putea fi folosite.

În timpul celui de-al doilea război mondial al New York existau 4 300 de funcționari care se ocupau exclusiv cu activitatea de detectare a scrierilor ascunse din trîmțerile poștale. Toate mesajele care conțineau texte oarecum forțate, neîndeajuns de clare, suspecte din anumite puncte de vedere, erau examinate cu maximum de atenție.

Din punct de vedere lingvistic există două metode de a trimite mesaje cu caracter suspect: semagramele și codurile deschise. La rîndul lor, codurile deschise pot fi și ele de trei feluri: codul-jargon, cifrul nul și sistemele geometrice de tipul grătarului. În codul-jargon un anumit cuvînt, de obicei foarte banal, înlocuiește termenul real dintr-un text care se vrea cit

mai obișnuit și nevinovat posibil. Fraze în aparență nevinovate, de tipul „L-am vizitat pe omul cu care ai luat masa săptămîna trecută” sau „Joe a fost dus la spital”, pot însemna că Joe a fost arestat etc. De obicei, în asemenea situații este bine să se verifice autenticitatea celor conținute în scrisoare, deoarece, așa cum au dovedit-o multe cazuri, mai ales în timpul celui de-al doilea război mondial, în astfel de scrisori se pot ascunde mesaje deosebit de periculoase. Astfel, proprietara unui magazin de păpuși scria că: „O păpușă stricată, îmbrăcată cu o rochie de culoarea ierbii, va fi reparată pînă la începutul lui februarie”. În realitate, prin acest mesaj se comunica că „Crucișătorul ușor Honolulu va fi reparat pînă la începutul lunii februarie”.

Cifrul nul constă în aceea că numai anumite cuvînte sau litere din textul respectiv au semnificație pentru adresant, cum ar fi, de exemplu, fiecare al cincilea cuvînt sau prima, a doua etc. literă din fiecare cuvînt și așa mai departe, restul textului servind doar la ascunderea mesajului.

Un astfel de text este următorul:

Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on byproducts, ejecting sueta and vegetable oils¹.

Acest text greoi și amuzant al unei telegrame interceptate conținea însă următorul mesaj: Pershing sails from N.Y., June 1. (Nava Pershing pleacă din New York pe 1-ia Iunie). Mesajul îl forma fiecare a doua literă din cuvintele telegramii.

A doua categorie de mesaje ascunse din punct de vedere lingvistic o constituie semagramele (sema în limba greacă = semn). Semagrama este o steganogramă în care textul cifrat este substituit prin orice alt semn, exceptînd literele și numerele. Așa, de exemplu, un desen, reprezentînd două obiecte sau figuri, poate fi făcut din liniile și punctele alfabetului Morse, conținînd și ora la care o anumită acțiune urmează să aibă loc.

¹ În limba română: „Se pare că protestul neutrilor nu este luat în seamă. El este complet ignorat. Isman a fost lovit greu. Blocada afectează, pretext pentru embargoul asupra produselor secundare, uleiurile vegetale și altele”.

Steganografia tehnologică la început a constatat mai ales din depistarea scrierilor făcute cu ajutorul cernelurilor invizibile.

Cernelurile secrete sînt de două feluri: lichide organice și produse chimice simpatice.

Lichidele organice ca urina, laptele, oțetul și sucurile de fructe pot fi făcute vizibile printr-o încălzire ușoară. Deși sînt cunoscute din antichitate și sînt foarte vulnerabile, datorită faptului că pot fi procurate ușor, fiind la îndemîna oricui și oricînd, se folosesc și astăzi.

Cernelurile simpatice sînt soluții din diferite chimicale care, cînd se usucă, devin incolore, dar reacționează, devenind vizibile, cu o altă substanță chimică numită agent. De exemplu, dacă se scrie cu sulfat de fier, nimic nu devine vizibil pînă cînd nu se dă peste scrisoare cu cianură de potasiu și, din reacție, rezultă ferrocianura ferică, de culoare albastră; subacetatul de plumb devine vizibil numai în reacție cu sulfhidrat de sodiu; sulfatul de cupru devine vizibil în reacție cu vapori de amoniac etc.

Pentru a testa existența cernelii simpatice, lucrătorul din laborator, cu ajutorul cîtorva pensule, legate într-un mînunchi și înmuiate în agenți diferiți, trage o linie în diagonală peste scrisoare. Se folosesc agenți foarte diferiți, încît deseori apar amprente și picături de sudoare. Pe de altă parte, anumite cerneluri specifice nu apar, ci rămîn în continuare ascunse. Pentru a înlătura liniile respective, scrisoarea este recondiționată pe cale chimică. Scrisorile sînt verificate, de asemenea, și cu ajutorul razelor infraroșii și ultraviolete.

Diferite scrieri cu ajutorul unor substanțe sînt invizibile la lumina zilei sau a unor becuri, dar devin vizibile la lumină ultravioletă.

Lumina infraroșie poate diferenția scrisul cu culori care nu pot fi distinse la lumina obișnuită, așa cum ar fi, de exemplu, un mesaj scris cu culoare verde pe un timbru verde.

Bineînțeles, împotriva acestor metode de depistare a scrierilor ascunse s-au luat o serie de contramăsuri. Una dintre acestea a fost despicarea în două a foil de hîrtie și scrierea mesajului pe partea interioară, după care cele două părți se re-

lipeau. Cerneala fiind în interior, nici un agent nu o făcea vizibilă. Această metodă a fost descoperită cînd un spion german, neastent, a folosit prea multă cerneală și aceasta a trecut prin hîrtie.

Neajunsul în tehnica cernelurilor simpatice este acela că nu permite trimiterea unui volum mai mare de informații.

O altă metodă de a transmite o cantitate mare de informații este de a puncta toate literele, care constituie un mesaj, dintr-un ziar cu ajutorul unei soluții de antracină în alcool. Punctele sînt invizibile în condiții normale, dar apar cînd sînt expuse la lumină ultravioletă.

În cazul de față, neajunsul este acela că ziarele ajung cu întîrziere la destinație, existînd și pericolul de a se rătăci sau rupe.

Un procedeu deosebit este micropunctul. În 1941, americanii au descoperit primul micropunct, care nu este altceva decît fotografia, redusă la scară, a unui mesaj, document etc.

În faza inițială, tehnica micropunctului implica două etape: la început, se făcea o fotografie a mesajului de mărimea unui timbru, apoi se fotografia din nou această imagine printr-un microscop întors, după care se developa negativul fotografiei. Punctul obținut se lua cu ajutorul unui ac și era inserat în textul mască al scrisorii de dragoste, de afaceri etc.

Primul micropunct descoperit conținea o întrebare demnă de acest eveniment și anume: „Unde se fac experiențe cu uraniu?”.

CUPRINSUL

| | <i>Pag.</i> |
|---|-------------|
| Din partea redacției | 3 |
| Nașterea criptologiei : | 5 |
| Ridicarea vestului | 23 |
| Contribuția diletanților | 39 |
| Profesorul, soldatul și omul de geniu | 57 |
| „Camera 40” | 69 |
| Războiul interceptărilor | 85 |
| Secretul de vânzare | 91 |
| Conșieri și spioni | 107 |

Responsabil de editură căpitău CONSTANTIN GĂDEA
Corector: d. RADU STOIAN

Dată la cules XLXIII

B.T. la XLXIII

Tiraj 1 000, din care 1 000 exemplare hirtie semivellină
și 100 exemplare hirtie velină, format 16/91 X 85